

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-261550

(43)Date of publication of application : 24.09.1999

(51)Int.Cl.

H04L 9/32

G06F 12/14

G06F 17/21

G09C 1/00

(21)Application number : 10-271541

(71)Applicant : TOSHIBA CORP

(22)Date of filing : 25.09.1998

(72)Inventor : ONO KAZUTERU

(30)Priority

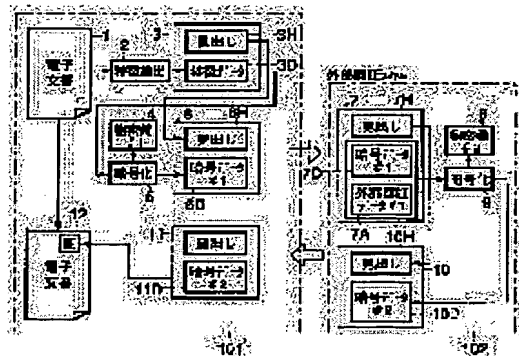
Priority number : 10 717 Priority date : 06.01.1998 Priority country : JP

(54) SYSTEM AND METHOD FOR PREVENTING ELECTRONIC DOCUMENT FORGERY

(57)Abstract:

PROBLEM TO BE SOLVED: To add an evidence capability to an electronic document and also to promote document computerization in a true sense.

SOLUTION: This system is provided with a characteristics extracting means 11 which extracts a characteristics and produces characteristics data, a 1st enciphering means 5 which enciphers the characteristics data with the 1st key of cryptograph of the 1st person concerned and produces 1st enciphered data, a 2nd enciphering means 9 which adds external authentication data including at least a date to the 1st enciphered data enciphers it with the 2nd key of cryptograph of an external authenticating person and produces 2nd enciphered data, and a means which authenticates the 2nd enciphered data as authentication data of the electronic document.



LEGAL STATUS

[Date of request for examination]

05.03.2002

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision
of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-261550

(43) 公開日 平成11年(1999) 9月24日

(51) IntCl.⁹
H 0 4 L 9/32
G 0 6 F 12/14
17/21
G 0 9 C 1/00
識別記号
3 1 0
6 4 0

F I
H 0 4 L 9/00
G 0 6 F 12/14
G 0 9 C 1/00
G 0 6 F 15/20
H 0 4 L 9/00
6 7 5 B
3 1 0 Z
6 4 0 B
5 7 0 M
6 7 3 D

審査請求 未請求 請求項の数37 O L (全 65 頁) 最終頁に続く

(21) 出願番号 特願平10-271541
(22) 出願日 平成10年(1998) 9月25日
(31) 優先権主張番号 特願平10-717
(32) 優先日 平10(1998) 1月6日
(33) 優先権主張国 日本 (J P)

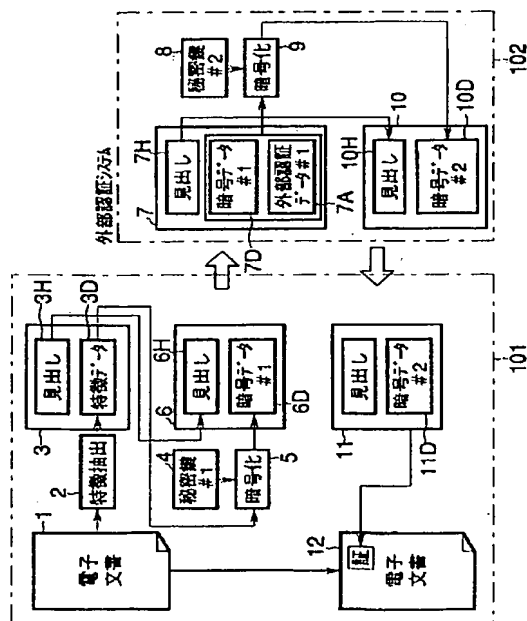
(71) 出願人 000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地
(72) 発明者 小野 和輝
東京都府中市東芝町1番地 株式会社東芝
府中工場内
(74) 代理人 弁理士 鈴江 武彦 (外6名)

(54) 【発明の名称】 電子文書の改竄防止システム及び方法

(57) 【要約】

【課題】 本発明は、電子文書に証拠能力を付与するとともに、真の意味での文書の電子化を推進することを可能とする。

【解決手段】 電子文書から特徴を抽出して特徴データを生成する特徴抽出手段11と、特徴データを第1の当事者の第1の暗号鍵で暗号化し、第1の暗号化データを生成する第1の暗号化手段5と、第1の暗号化データに、少なくとも日付を含む外部認証データを付加し、これを外部認証者の第2の暗号鍵で暗号化して第2の暗号化データを生成する第2の暗号化手段9と、第2の暗号化データを電子文書の認証データとする手段S14とを備えた電子文書の改竄防止システム。



【特許請求の範囲】

【請求項1】 電子文書から特徴を抽出して特徴データを生成する特徴抽出手段と、

前記特徴データを第1の暗号鍵で暗号化して第1の暗号化データを生成する第1の暗号化手段と、

前記第1の暗号化データに、外部認証データを付加し、これを第2の暗号鍵で暗号化して第2の暗号化データを生成する第2の暗号化手段と、

前記第2の暗号化データを前記電子文書の認証データとする手段とを備える電子文書の改竄防止システム。

【請求項2】 電子文書から特徴を抽出して特徴データを生成する特徴抽出手段、前記特徴データを第1の暗号鍵で暗号化して第1の暗号化データを生成する第1の暗号化手段、前記第1の暗号化データを送信するとともに認証データを受信する第1の通信手段、および前記認証データを前記電子文書に対応させる手段とを備える文書認証システムと、

前記第1の通信手段にて送信される前記第1の暗号化データに、少なくとも日付を含む外部認証データを付加し、これを第2の暗号鍵で暗号化して第2の暗号化データを生成する第2の暗号化手段、および前記第1の暗号化データを受信するとともに前記第2の暗号化データを認証データとして前記文書認証システムに送信する第2の通信手段を備える外部認証システムと、を備えた電子文書の改竄防止システム。

【請求項3】 前記第1の暗号化データを第3の暗号鍵で暗号化して第3の暗号化データを生成する第3の暗号化手段を備え、前記第2の暗号化手段は、前記第1の暗号化データに代えて、前記第3の暗号化データに外部認証データを付加して第2の暗号鍵で暗号化して第2の暗号化データを生成することを特徴とする請求項1又は2記載の電子文書の改竄防止システム。

【請求項4】 前記第2の暗号化データを、前記第2の暗号鍵とは異なる第4の暗号鍵で暗号化して第4の暗号化データを生成し、前記認証データとする第4の暗号化手段とを備えることを特徴とする請求項1、2又は3記載の電子文書の改竄防止システム。

【請求項5】 認証対象の電子文書に対応する認証データから第2の暗号化データを取り出し、これを第2の暗号鍵に対応する第2の公開鍵で復号化する第2の復号化手段と、

前記第2の復号化手段により復号化されたデータから第1の暗号化データを取り出し、これを第1の暗号鍵に対応する第1の公開鍵で復号化する第1の復号化手段と、前記電子文書から特徴を抽出して照会用特徴データを生成する特徴抽出手段と、

前記第1の復号化手段により復号化されたデータから特徴データを取り出し、前記照会用特徴データと照合する照合手段とを備えたことを特徴とする認証文書確認システム。

【請求項6】 請求項5において、前記第2の復号化手段により復号化されたデータから第3の暗号化データを取り出し、これを第3の暗号鍵に対応する第3の公開鍵で復号化する第3の復号化手段を設け、

前記第1の復号化手段は前記第3の復号化手段により復号化されたデータから第1の暗号化データを取り出し、これを第1の暗号鍵に対応する第1の公開鍵で復号化することを特徴とする認証文書確認システム。

【請求項7】 特徴抽出対象データを1単位ずつ読み出して、読み出した値を順に規定の単位数だけ加算してなる合計値を順次並べて第1の合計値列とする第1列生成手段と、

この1単位ずつ読み出した値に対して前記規定の単位数だけ隔てた関係となる1単位ずつ読み出した値を加算し、この加算した値に対して前記関係となる1単位ずつ読み出した値を加算し、この加算を繰り返し、合計加算回数として前記規定の単位数回の加算を行って得られる合計値を順次並べて第2の合計値列とする第2列生成手段と、

前記第1の合計値列及び前記第2の合計値列を特徴データとして出力する手段とを備えたことを特徴とする特徴抽出装置。

【請求項8】 前記第1の合計値列を1単位ずつ読み出して、読み出した値を順に規定の単位数だけ加算してなる合計値を順次並べて第3の合計値列とする第3列生成手段と、

前記第2の合計値列を1単位ずつ読み出して、読み出した値を順に規定の単位数だけ加算してなる合計値を順次並べて第4の合計値列とする第4列生成手段と、

前記第3の合計値列及び前記第4の合計値列を特徴データとして出力する手段とを備えたことを特徴とする請求項7記載の特徴抽出装置。

【請求項9】 指紋読取手段と、

前記指紋読取手段で読み取った指紋データから特徴抽出を行い指紋特徴データを生成する指紋特徴抽出手段と、前記指紋特徴データ及びパスワードから暗号鍵を生成する暗号鍵生成手段と、

前記指紋特徴データ、パスワード及び乱数値から秘密鍵及び公開鍵を生成する秘密鍵公開鍵生成手段と、

前記暗号鍵で前記暗号鍵自身と前記秘密鍵をそれぞれ暗号化する暗号化手段と、

前記暗号化手段で暗号化したデータ、指紋データ及びパスワードを本人認証データとする手段とを備えたことを特徴とする本人認証データ生成システム。

【請求項10】 前記請求項9に記載された本人認証データ生成システムで生成した前記本人認証データ中のパスワードと、入力されたパスワードとを照合するパスワード照合手段と、

指紋読取手段と、

両パスワードが一致した場合には、前記指紋読取手段で

指紋読み取りを行い、前記本人認証データ中の指紋データと、前記指紋読取手段にて読み取られた指紋データとを照合する指紋照合手段と、
指紋照合が一致した場合には、前記本人認証データ中の指紋データから特徴抽出を行い指紋特徴データを生成する指紋特徴抽出手段と、
前記指紋特徴抽出手段にて生成された指紋特徴データ及びパスワードから暗号鍵を生成する暗号鍵生成手段と、
この生成された暗号鍵により本人認証データ内の暗号化された暗号鍵を復号して、前記生成された暗号鍵と復号した暗号鍵とを照合する暗号鍵照合手段と、
暗号鍵照合が一致した場合には、この暗号鍵を用いて前記本人認証データ中の暗号化した秘密鍵を復号する秘密鍵復号手段とを備えた秘密鍵復号システム。

【請求項11】 指紋読取手段と、

前記指紋読取手段から読み取られる指紋データの境界を検出する境界検出手段と、
前記境界検出手段により境界検出された指紋データをエンボス処理するエンボス手段と、
前記エンボス手段によりエンボス処理された指紋データを輪郭トレースする輪郭トレース手段とを備えたことを特徴とする指紋データ抽出装置。

【請求項12】 前記請求項11に記載された指紋データ抽出装置から抽出された指紋データから複数の矩形領域を取り出す領域取出手段と、
前記矩形領域のデータと予め登録した複数パターンとを比較し、何れかのパターンとマッチングするか否かを判定するパターンマッチング手段と、
マッチングしたパターンに対応する数値を数列として並べ、当該数列を指紋特徴データとする手段とを備えたことを特徴とする指紋特徴抽出装置。

【請求項13】 電子文書から特徴を抽出して特徴データを生成する特徴抽出ステップと、
前記特徴データを第1の当事者の第1の暗号鍵で暗号化し、第1の暗号化データを生成する第1の暗号化ステップと、
前記第1の暗号化データに、少なくとも日付を含む外部認証データを付加し、これを外部認証者の第2の暗号鍵で暗号化して第2の暗号化データを生成する第2の暗号化ステップと、
前記第2の暗号化データを前記電子文書の認証データとするステップとを有することを特徴とする電子文書の改竄防止方法。

【請求項14】 電子文書から抽出したデータを第1の暗号鍵で暗号化して第1の暗号化データを生成する文書認証システムと、受信データを第2の暗号鍵で暗号化して第2の暗号化データを生成する外部認証システムとが通信回線で接続される電子文書の改竄防止システムであって、
文書認証システムにて生成した前記第1の暗号化データ

を、前記通信回線を介して前記外部認証システムに送信し、

外部認証システムでは、受信した前記第1の暗号化データに、少なくとも日付を含む外部認証データを付加し、これを第2の暗号鍵で暗号化して第2の暗号化データを生成し、この第2の暗号化データを認証データとして前記文書認証システムに送信し、

文書認証システムでは、受信した前記第2の暗号化データを認証データとして前記電子文書に対応させることを特徴とする電子文書の改竄防止方法。

【請求項15】 第1の文書認証システムにて、電子文書から抽出したデータを第1の暗号鍵で暗号化して第1の暗号化データを生成し、第2の文書認証システムに送信し、

第2の文書認証システムにて、前記第1の文書認証システムより送信された前記第1の暗号化データを第3の暗号鍵で暗号化して第3の暗号化データを生成し、外部認証システムに送信し、

外部認証システムにて、前記第2の文書認証システムより送信された前記第3の暗号化データに外部認証データを付加し、これを第2の暗号鍵で暗号化して第2の暗号化データを生成し、少なくとも前記第1の文書認証システムに送信し、

当該第1の文書認証システムにて、受信した前記第2の暗号化データを認証データとして前記電子文書に対応させることを特徴とする電子文書の改竄防止方法。

【請求項16】 前記請求項1、2又は3記載の電子文書の改竄防止システムにて生成された前記認証データから前記第2の暗号化データを取出し、これを前記第2の秘密鍵に対応する第2の公開鍵で復号化する第2の復号化ステップと、

前記第2の復号化ステップにより復号化されたデータから前記第1の暗号化データを取出し、これを前記第1の秘密鍵に対応する第1の公開鍵で復号化する第1の復号化ステップと、

前記電子文書から特徴を抽出して照合用特徴データを生成する特徴抽出ステップと、

前記第1の復号化ステップにより復号化されたデータから前記特徴データを取出し、これを前記照合用特徴データと照合する照合ステップと、

前記照合ステップによる照合結果と、前記第2の復号化手段により復号化されたデータから取り出された前記外部認証データによって、外部認証者による認証の事実及び認証の日付を出力するステップとを有することを特徴とする認証文書確認方法。

【請求項17】 電子文書から特徴を抽出して特徴データを生成する特徴抽出手段と、
前記特徴データを第1の当事者の第1の暗号鍵で暗号化し、第1の暗号化データを生成する第1の暗号化手段と、

前記第 1 の暗号化データに、少なくとも日付を含む外部認証データが付加され、これが外部認証者の第 2 の暗号鍵によって暗号化されてなる第 2 の暗号化データが入力されるとともに、この第 2 の暗号化データを前記電子文書の認証データとする手段として、コンピュータを機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項 1 8】 前記請求項 1, 2 又は 3 記載の電子文書の改竄防止システムにて生成された前記認証データから前記第 2 の暗号化データを取出し、これを前記第 2 の秘密鍵に対応する第 2 の公開鍵で復号化する第 2 の復号化手段と、

前記第 2 の復号化手段により復号化されたデータから前記第 1 の暗号化データを取出し、これを前記第 1 の秘密鍵に対応する第 1 の公開鍵で復号化する第 1 の復号化手段と、

前記電子文書から特徴を抽出して照合用特徴データを生成する特徴抽出手段と、

前記第 1 の復号化手段により復号化されたデータから前記特徴データを取出し、これを前記照合用特徴データと照合する照合手段と、

前記照合手段による照合結果と、前記第 2 の復号化手段により復号化されたデータから取り出された前記外部認証データによって、外部認証者による認証の事実及び認証の日付を出力する手段として、コンピュータを機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項 1 9】 電子文書から特徴が抽出されて特徴データが生成され、

次に、前記特徴データが第 1 の当事者の第 1 の暗号鍵で暗号化され、第 1 の暗号化データが生成され、

次に、前記第 1 の暗号化データに、少なくとも日付を含む外部認証データが付加されて、これが外部認証者の第 2 の暗号鍵で暗号化して第 2 の暗号化データが生成され、

最終的に、前記第 2 の暗号化データからなる構造を有するデータが記録されたコンピュータ読み取り可能な記録媒体。

【請求項 2 0】 電子文書から特徴が抽出されて特徴データが生成され、

次に、前記特徴データが第 1 の当事者の第 1 の暗号鍵で暗号化され、第 1 の暗号化データが生成され、

次に、前記第 1 の暗号化データが第 2 の当事者の第 3 の暗号鍵で暗号化され、第 3 の暗号化データが生成され、

次に、前記第 3 の暗号化データに、少なくとも日付を含む外部認証データが付加されて、これが外部認証者の第 2 の暗号鍵で暗号化して第 2 の暗号化データが生成され、

最終的に、前記第 2 の暗号化データからなる構造を有するデータが記録されたコンピュータ読み取り可能な記録

媒体。

【請求項 2 1】 認証付き電子文書から電子文書を取り出して、これに変更を加えて、新たな電子文書を生成する文書変更手段と、

前記認証付き電子文書から取り出された元の電子文書と前記新たな電子文書との変更点を抽出して変更箇所データを取得する差分抽出手段と、

前記変更箇所データと前記新たな電子文書とをそれぞれ変更者認証する変更者認証手段と、

10 前記変更者認証手段により認証された各データを外部の認証システムに送出するとともに、それぞれを外部認証された認証データを受け取って、受け取った各認証データ及び前記新たな電子文書に基づいて、認証付き変更箇所データと新たな認証付き電子文書を生成する認証手段とを備えたことを特徴とする電子文書の改竄防止システム。

【請求項 2 2】 前記変更者認証手段は、

前記変更箇所データ及び又は前記新たな電子文書から特徴抽出して特徴データを出力する特徴抽出手段と、

20 前記特徴データを、前記新たな電子文書を生成した変更者の暗号化鍵で暗号化して出力する暗号化手段とを備えたことを特徴とする請求項 2 1 記載の電子文書の改竄防止システム。

【請求項 2 3】 前記変更者認証手段は、

前記暗号化手段から出力されかつ前記新たな電子文書に対応する暗号化特徴データと、元の認証付き電子文書から取り出された以前の認証データとを結合して出力する結合手段を備えたことを特徴とする請求項 2 2 記載の電子文書の改竄防止システム。

30 【請求項 2 4】 前記変更者認証手段は、

前記特徴抽出手段により特徴抽出された特徴データと、元の認証付き電子文書から取り出された以前の認証データとを結合して出力する結合手段を備え、

前記暗号化手段の暗号化対象として、前記結合手段からの出力データを前記特徴データに代えて入力することを特徴とする請求項 2 2 記載の電子文書の改竄防止システム。

40 【請求項 2 5】 前記請求項 2 1 乃至 2 4 のうち何れか 1 項に記載された認証手段により生成された認証付き変更箇所データと認証付き電子文書とを含む変更済電子文書から、前記認証付き変更箇所データ及び前記認証付き電子文書を取り出す分離手段と、

前記請求項 2 1 乃至 2 4 のうち何れか 1 項に記載された文書変更手段、差分抽出手段、変更者認証手段及び認証手段と、

50 前記認証手段により生成された新たな認証付き変更箇所データ及び新たな認証付き電子文書と、前記分離手段で分離された元の認証付き変更箇所データとに基づき、新たな変更済電子文書を生成する結合手段とを備えたことを特徴とする電子文書の改竄防止システム。

【請求項26】 前記請求項21乃至24のうち何れか1項に記載された前記変更者認証手段により認証された各データを受け取る受入手段と、
前記各データそれぞれに、少なくとも日付データ及び認証実行識別情報を結合する結合手段と、
この結合手段により結合された各データを外部認証機関の暗号鍵によって暗号化して、外部認証された認証データを作成する暗号化手段とを備えたことを特徴とする電子文書の外部認証システム。

【請求項27】 前記請求項26に記載の外部認証システムにより外部認証された認証データを、外部認証機関の復号鍵で復号する復号化手段と、
前記復号化手段により復号された認証データから、前記日付データ及び前記認証実行識別情報を取り出すデータ取出手段とを備えたことを特徴とする認証文書確認システム。

【請求項28】 前記請求項26に記載の外部認証システムにより外部認証された認証データが前記請求項23に対応しかつ電子文書に対応するものである場合に、
前記復号化手段により復号された認証データから、前記以前の認証データを取り出す認証データ取出手段を備えたことを特徴とする請求項27記載の認証文書確認システム。

【請求項29】 前記復号化手段により復号された認証データのうち、前記請求項22の暗号化手段で暗号化された暗号データが入力されるとともに、当該暗号データを変更者の復号鍵で復号して特徴データを取り出す第2の復号化手段と、
前記請求項21の文書変更手段で得られた新たな電子文書から特徴抽出して比較用特徴データを出力する特徴抽出手段と、
前記第2の復号化手段で得られた特徴データと、前記特徴抽出手段で得られた比較用特徴データとを比較する照合手段とを備えたことを特徴とする請求項28記載の認証文書確認システム。

【請求項30】 前記請求項26に記載の外部認証システムにより外部認証された認証データが前記請求項24に対応しかつ電子文書に対応するものである場合に、
前記復号化手段により復号された認証データを変更者の復号鍵で復号する第2の復号化手段と、
前記第2の復号化手段で復号化された認証データから、前記以前の認証データを取り出す認証データ取出手段とを備えたことを特徴とする請求項27記載の認証文書確認システム。

【請求項31】 前記第2の復号化手段で復号化された認証データから、特徴データを取り出す分離手段と、
前記請求項21の文書変更手段で得られた新たな電子文書から特徴抽出して比較用特徴データを出力する特徴抽出手段と、
前記分離手段で得られた特徴データと、前記特徴抽出手

段で得られた比較用特徴データとを比較する照合手段とを備えたことを特徴とする請求項30記載の認証文書確認システム。

【請求項32】 前記請求項26に記載の外部認証システムにより外部認証された認証データが前記請求項22に対応しかつ前記変更箇所データに対応するものである場合に、

前記復号化された認証データのうち、前記請求項22の暗号化手段で暗号化された暗号データが入力されるとともに、当該暗号データを変更者の復号鍵で復号して特徴データを取り出す第2の復号化手段と、

前記請求項21の差分抽出手段で得られた変更箇所データから特徴抽出して比較用特徴データを出力する特徴抽出手段と、

前記第2の復号化手段で得られた特徴データと、前記特徴抽出手段で得られた比較用特徴データとを比較する照合手段とを備えたことを特徴とする請求項27記載の認証文書確認システム。

【請求項33】 前記請求項25に記載された電子文書の改竄防止システムにより作成された変更済電子文書の変更部分についての認証確認を行うシステムであって、
前記請求項28又は30の認証文書確認システムと、前記請求項32の認証文書確認システムとを備えるとともに、

複数回の変更を受けた最終的な変更済電子文書における認証付き電子文書から、最終変更回に関する認証データを取り出し、まずこれを前記請求項26に記載の外部認証システムにより外部認証された認証データとして前記請求項28又は30の認証文書確認システムに入力し、
最終変更回以外の各回については、前記請求項28又は30の認証文書確認システムから出力される前記以前の認証データを、前記請求項26に記載の外部認証システムにより外部認証された認証データとして、順次、前記請求項28又は30の認証文書確認システムに入力し、
また、複数回の変更を受けた最終的な変更済電子文書から、各回の認証付き変更箇所データを取り出し、この認証付き変更箇所データを変更箇所データ及び前記請求項26に記載の外部認証システムにより外部認証された認証データに分離して、前記請求項32の認証文書確認システムに入力し、

前記請求項28又は30の認証文書確認システムから得られた日付データ及び認証実行識別情報と、前記請求項32の認証文書確認システムから得られた日付データ及び認証実行識別情報とを各変更回毎に照合することを特徴とする変更済電子文書の認証確認システム。

【請求項34】 前記請求項29又は31の認証文書確認システムを備えるとともに、
最終的な変更済電子文書に含まれる認証付き電子文書から取り出された認証データ及び新たな電子文書を、前記請求項28又は30の認証文書確認システムに代えて

前記請求項29又は31の認証文書確認システムに入力することを特徴とする請求項33記載の変更済電子文書の認証確認システム。

【請求項35】 認証付き電子文書から電子文書を取り出して、これに変更を加えて、新たな電子文書を生成する文書変更手段と、

前記認証付き電子文書から取り出された元の電子文書と前記新たな電子文書との変更点を抽出して変更箇所データを取得する差分抽出手段と、

前記変更箇所データと前記新たな電子文書とをそれぞれ変更者認証する変更者認証手段と、

前記変更者認証手段により認証された各データを外部の認証システムに送出するとともに、それぞれを外部認証された認証データを受け取って、受け取った各認証データ及び前記新たな電子文書に基づいて、認証付き変更箇所データと新たな認証付き電子文書を生成する認証手段として、コンピュータを機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項36】 前記変更者認証手段は、前記変更箇所データ及び又は前記新たな電子文書から特徴抽出して特徴データを出力する特徴抽出手段と、前記特徴データを、前記新たな電子文書を生成した変更者の暗号化鍵で暗号化して出力する暗号化手段として、コンピュータを機能させるためのプログラムを記録したコンピュータ読み取り可能な請求項35記載の記録媒体。

【請求項37】 前記請求項26に記載の外部認証システムにより外部認証された認証データを、外部認証機関の復号鍵で復号する復号化手段と、

前記復号化手段により復号された認証データから、前記日付データ及び前記認証実行識別情報を取り出すデータ取出手段として、コンピュータを機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明はデータや文書等の電子文書の改竄を防止し、特に電子文書の証拠能力を確保する部分に特徴のある電子文書の改竄防止システム及び方法に関するものである。

【0002】

【従来の技術】従来から取引記録、品質記録あるいは契約書等の文書は、文書改竄の疑惑を防止する為に、黒インクやボールペン等を用いて紙上に記入し署名や捺印を行っている。

【0003】このように紙にインクで記載したものは、後に記載内容や日付を改竄しようとしても容易には改竄できない。紙は古くなると質が変化する為に、新しく偽の文書を作成しても判別が可能である。こうした紙とインクの特徴の為に、従来から重要文書は全て紙で保管さ

れている。

【0004】最近、電子署名技術が開発され、文書を作成した本人を証明する事ができるようになっている。この電子署名を説明する。

【0005】図53は電子文書に署名してその同一性を判定する従来の方法を示す図である。

【0006】同図に示すように、まず、電子文書201aから特徴抽出手段202で特徴データ203Dを取り出す。次に、この特徴データ203Dを秘密鍵204を用い、暗号化手段205により暗号化して暗号データ206Dを作成する。そして、この暗号データ206Dを元の電子文書201aと一緒にして署名済み電子文書201bとして受取人に送信する。

【0007】受取人は、受け取った電子文書201b'から暗号データ206Dを取り出して送信者の公開鍵216を使用し復号化手段217により特徴データ218Dを取り出す。一方、電子文書201b'から元の電子文書201aに相当する電子文書201a'を取り出し、さらに特徴抽出手段220により特徴データ221を取り出す。特徴データ221を先の特徴データ218Dと照合手段22により照合し本人の電子文書に相違無い事を確認する。

【0008】このような電子文書であれば、その文書作成者は間違いなく本人である事を確認できる。しかし、作成者本人であれば、作成済みの文書を自由に改変することが可能である。したがって、作成者本人が、例えばコンピュータの日付を故意にずらせて文書の作成日付を隠蔽化する等の問題を生じ得る。

【0009】ここで、特願平5-303773号公報に記載される「電子化文書処理システムおよびデジタル署名の生成方法」では、作成した文書に別の作者が一部変更を加えて、新しい文書にする時の認証方法が開示されている。

【0010】しかし、作成した電子文書を、作成に関わった作者等以外の利害の対立する者に対して証拠書類として使用することは、作成に関わった作者等が共謀して改竄を行なえば証拠改竄が可能となることから適切とはいえない。すなわち特願平5-303773号公報の方法は、文書を証拠書類として電子化させることには馴染まず、社内文書を社内で使用する場合に限った電子化といえる。

【0011】例えば製品の製造工程に従って、工程毎の担当者が、自分の担当工程に署名捺印を行なう組み立て記録等には適用できず、紙での運用となっている。また、定期検査の記録で、記録シートに数行の点検結果を追記して署名捺印を行なう場合にも、紙での運用になっていた。このような物は製品安全の事故に対して、検査記録を証拠とする必要があり、共謀すれば改竄できる電子文書では証拠とはなり得なかった為である。

【0012】

【発明が解決しようとする課題】このように文書作成者

本人は文書改竄を行う事ができるので、取引記録、品質記録あるいは契約書等の電子文書を本人が改竄していないことが証明できない。このため、現状のシステムでは電子文書に対する信用性は低く、重要書類は相変わらず紙で取り扱われている。

【0013】しかし、紙の文書は保管に多くの場所を必要とし、必要な文書を取り出すのに時間が掛かる。また、遠方に送る時に本紙と同じ証拠能力を持つ必要がある場合には、本紙を送る以外に方法が無い問題がある。

【0014】一方、最近のコンピュータの発達で文書がワープロなどで作成される様になると、紙の形で保管しておくよりも、電子文書として保管する方が便利である。たとえば保管場所を取らない、必要な文書の検索が容易である等の利点を有する為であり、このため文書の電子化が社会一般的に進んで来ている。

【0015】しかし、上記したように電子文書の証拠能力が不足している事から、重要文書の電子化ができず、たとえ電子化しても、証拠能力を有する紙文書が本紙として別途必要である。このため、重要文書に関しての保管場所が必要である等の問題は依然として解決されない。

【0016】本発明は、このような実情を考慮してなされたもので、本来紙文書の特徴である証拠能力を電子文書に付与するとともに、真の意味での文書の電子化を推進することを可能とし、ひいては、文書の保管場所の削減、文書の検索の効率化、本紙の文書の遠方への即時配達等を実現できる電子文書の改竄防止システム及び方法を提供することを目的とする。

【0017】また、本発明の他の目的は、複数人が複数時期に渡って一つの電子文書を作成する場合でも、変更文書を関係者全員で再承認する必要をなくしかつ文書改竄を防止して、紙文書の証拠能力以上の証拠能力を有する電子文書を作成可能とした電子文書の改竄防止システム及び方法を提供することにある。

【0018】

【課題を解決するための手段】本発明の骨子は、電子文書から抽出された特徴データを第1当事者の暗号鍵で暗号化し、さらにこの暗号化された特徴データを外部認証者の暗号鍵で暗号化してその結果得られた暗号データを電子文書の認証データとして用いるところにある。

【0019】このようにして得られる認証データは、他人によって改竄することはできないし、暗号化された特徴データを渡された悪意の外部認証者によっても改竄できない。つまり特徴データ自体に第1当事者の暗号がかけられているため、外部認証者がこれを改竄すれば電子文書が正当でないことが検出されるものである。さらに、一度外部認証された認証データは、外部認証者による暗号化のために、第1当事者本人によっても改竄することが不能となる。

【0020】一方、もとの電子文書を改竄した場合に

は、改竄電子文書からの特徴データと、認証データに含まれる特徴データとの比較により、その改竄の事実が検出される。

【0021】このように、本発明では、悪意の他人による場合はもちろんのこと、悪意の第1当事者、さらには悪意の外部認証者のいずれによる場合であっても、もし電子文書又は認証データが何れの段階で改竄されれば、どの段階で改竄が行われた場合であってもその改竄事実が検出される。

【0022】また、上記課題の解決は、より具体的には、以下のような解決手段により実現される。

【0023】まず、請求項1に対応する発明は、電子文書から特徴を抽出して特徴データを生成する特徴抽出手段と、特徴データを第1の暗号鍵で暗号化して第1の暗号化データを生成する第1の暗号化手段と、第1の暗号化データに、外部認証データを付加し、これを第2の暗号鍵で暗号化して第2の暗号化データを生成する第2の暗号化手段と、第2の暗号化データを電子文書の認証データとする手段とを備える電子文書の改竄防止システムである。

【0024】本発明はこのような手段を設けたので、本来紙文書の特徴である証拠能力を電子文書に付与するとともに、真の意味での文書の電子化を推進することを可能とし、ひいては、文書の保管場所の削減、文書の検索の効率化、本紙の文書の遠方への即時配達等を実現することができる。

【0025】次に、請求項2に対応する発明は、電子文書から特徴を抽出して特徴データを生成する特徴抽出手段、特徴データを第1の暗号鍵で暗号化して第1の暗号化データを生成する第1の暗号化手段、第1の暗号化データを送信するとともに認証データを受信する第1の通信手段、および認証データを電子文書に対応させる手段とを備える文書認証システムと、第1の通信手段にて送信される第1の暗号化データに、少なくとも日付を含む外部認証データを付加し、これを第2の暗号鍵で暗号化して第2の暗号化データを生成する第2の暗号化手段、および第1の暗号化データを受信するとともに第2の暗号化データを認証データとして文書認証システムに送信する第2の通信手段を備える外部認証システムと、を備えた電子文書の改竄防止システムである。

【0026】本発明はこのような手段を設けたので、請求項1の発明と同様な効果が得られる他、通信回線を用いることで、第1の当事者と外部認証者と間で認証データ作成作業を便利かつ短時間に進めることができる。

【0027】次に、請求項3に対応する発明は、請求項1又は2に対応する発明において、第1の暗号化データを第3の暗号鍵で暗号化して第3の暗号化データを生成する第3の暗号化手段を備え、第2の暗号化手段は、第1の暗号化データに代えて、第3の暗号化データに外部認証データを付加して第2の暗号鍵で暗号化して第2の

暗号化データを生成する電子文書の改竄防止システムである。

【0028】本発明はこのような手段を設けたので、請求項1の発明と同様な効果が得られる他、認証データに第2の当事者の暗号鍵による暗号化を加え、この電子文書を第1の当事者、第2の当事者及び外部認証者の三者の認証になる電子傾斜区処とすることができる。

【0029】次に、請求項4に対応する発明は、請求項1～3に対応する発明において、第2の暗号化データを、第2の暗号鍵とは異なる第4の暗号鍵で暗号化して第4の暗号化データを生成し、認証データとする第4の暗号化手段を備える電子文書の改竄防止システムである。

【0030】本発明はこのような手段を設けたので、例えば認証データ作成から長期間をへて、技術の進歩でその暗号が解読される可能性が生じたような場合でも、請求項1～3のうち何れか1項記載の電子文書の改竄防止システムにて生成された第2の暗号化データについて、再度の暗号化による外部認証者の再認証を行うことができ、電子文書の改竄に対する防御性を維持することができる。

【0031】次に、請求項5に対応する発明は、認証対象の電子文書に対応する認証データから第2の暗号化データを取り出し、これを第2の暗号鍵に対応する第2の公開鍵で復号化する第2の復号化手段と、第2の復号化手段により復号化されたデータから第1の暗号化データを取り出し、これを第1の暗号鍵に対応する第1の公開鍵で復号化する第1の復号化手段と、電子文書から特徴を抽出して照会用特徴データを生成する特徴抽出手段と、第1の復号化手段により復号化されたデータから特徴データを取り出し、照会用特徴データと照合する照合手段とを備えた認証文書確認システムである。

【0032】本発明はこのような手段を設けたので、本来紙文書の特徴である証拠能力が付与された電子文書について、その認証事実及び認証日を確認するとともに、真の意味での文書の電子化を推進するのに貢献できるシステムを提供することができる。これにより、ひいては、文書の保管場所の削減、文書の検索の効率化、本紙の文書の遠方への即時配達等を実現することができる。

【0033】次に、請求項6に対応する発明は、請求項5に対応する発明において、第2の復号化手段により復号化されたデータから第3の暗号化データを取り出し、これを第3の暗号鍵に対応する第3の公開鍵で復号化する第3の復号化手段を設け、第1の復号化手段は第3の復号化手段により復号化されたデータから第1の暗号化データを取り出し、これを第1の暗号鍵に対応する第1の公開鍵で復号化する認証文書確認システムである。

【0034】本発明はこのような手段を設けたので、第2の当事者を交えた電子契約書についても、請求項5の発明と同様な効果を得ることができる。

【0035】次に、請求項7に対応する発明は、特徴抽出対象データを1単位ずつ読み出して、読み出した値を順に規定の単位数だけ加算してなる合計値を順次並べて第1の合計値列とする第1列生成手段と、この1単位ずつ読み出した値に対して規定の単位数だけ隔てた関係となる1単位ずつ読み出した値を加算し、この加算した値に対して関係となる1単位ずつ読み出した値を加算し、この加算を繰り返し、合計加算回数として規定の単位数回の加算を行って得られる合計値を順次並べて第2の合計値列とする第2列生成手段と、第1の合計値列及び第2の合計値列を特徴データとして出力する手段とを備えた特徴抽出装置である。

【0036】本発明はこのような手段を設けたので、こうして得られた特徴データのみからではもとの電子文書を再現できず、その改変を行えばその旨を検出でき、かつ、もとの電子文書を大幅にデータ圧縮した特徴データを生成することができる。

【0037】次に、請求項8に対応する発明は、請求項7に対応する発明において、第1の合計値列を1単位ずつ読み出して、読み出した値を順に規定の単位数だけ加算してなる合計値を順次並べて第3の合計値列とする第3列生成手段と、第2の合計値列を1単位ずつ読み出して、読み出した値を順に規定の単位数だけ加算してなる合計値を順次並べて第4の合計値列とする第4列生成手段と、第3の合計値列及び第4の合計値列を特徴データとして出力する手段とを備えた特徴抽出装置である。

【0038】本発明はこのような手段を設けたので、請求項7の発明と同様な効果が得られる他、特徴データをより圧縮することができる。

【0039】次に、請求項9に対応する発明は、指紋読取手段と、指紋読取手段で読み取った指紋データから特徴抽出を行い指紋特徴データを生成する指紋特徴抽出手段と、指紋特徴データ及びパスワードから暗号鍵を生成する暗号鍵生成手段と、指紋特徴データ、パスワード及び乱数値から秘密鍵及び公開鍵を生成する秘密鍵公開鍵生成手段と、暗号鍵で暗号鍵自身と秘密鍵をそれぞれ暗号化する暗号化手段と、暗号化手段で暗号化したデータ、指紋データ及びパスワードを本人認証データとする手段とを備えた本人認証データ生成システムである。

【0040】本発明はこのような手段を設けたので、指紋等を用いて有効な本人認証データを作成することができる。なお、本システムで作成した本人認証データは、例えば文書改竄防止システムや認証文書確認システムの起動時の本人確認用のデータとすることができる。

【0041】次に、請求項10に対応する発明は、請求項9に記載された本人認証データ生成システムで生成した本人認証データ中のパスワードと、入力されたパスワードとを照合するパスワード照合手段と、指紋読取手段と、両パスワードが一致した場合には、指紋読取手段で指紋読み取りを行い、本人認証データ中の指紋データ

と、指紋読取手段にて読み取られた指紋データとを照合する指紋照合手段と、指紋照合が一致した場合には、本人認証データ中の指紋データから特徴抽出を行い指紋特徴データを生成する指紋特徴抽出手段と、指紋特徴抽出手段にて生成された指紋特徴データ及びパスワードから暗号鍵を生成する暗号鍵生成手段と、この生成された暗号鍵により本人認証データ内の暗号化された暗号鍵を復号して、生成された暗号鍵と復号した暗号鍵とを照合する暗号鍵照合手段と、暗号鍵照合が一致した場合には、この暗号鍵を用いて本人認証データ中の暗号化した秘密鍵を復号する秘密鍵復号手段とを備えた秘密鍵復号システムである。

【0042】本発明はこのような手段を設けたので、例えば文書改竄防止システムや認証文書確認システムの起動時に本人を高い確実性をもって確認することができる。

【0043】次に、請求項11に対応する発明は、指紋読取手段と、指紋読取手段から読み取られる指紋データの境界を検出する境界検出手段と、境界検出手段により境界検出された指紋データをエンボス処理するエンボス手段と、エンボス手段によりエンボス処理された指紋データを輪郭トレースする輪郭トレース手段とを備えた指紋データ抽出装置である。

【0044】本発明はこのような手段を設けたので、計算機で扱うことのできるデジタルデータとして指紋を抽出することができる。

【0045】次に、請求項12に対応する発明は、請求項11に記載された指紋データ抽出装置から抽出された指紋データから複数の矩形領域を取り出す領域取出手段と、矩形領域のデータと予め登録した複数のパターンとを比較し、何れかのパターンとマッチングするか否かを判定するパターンマッチング手段と、マッチングしたパターンに対応する数値を数列として並べ、当該数列を指紋特徴データとする手段とを備えた指紋特徴抽出装置である。

【0046】本発明はこのような手段を設けたので、効果的に指紋データから指紋特徴データを抽出することができる。

【0047】次に、請求項13に対応する発明は、請求項1の発明を方法発明としたものであり、請求項1の発明と同様な効果を奏する。

【0048】次に、請求項14に対応する発明は、請求項2の発明を方法発明としたものであり、請求項2の発明と同様な効果を奏する。

【0049】次に、請求項15に対応する発明は、請求項3の発明を方法発明としたものであり、請求項3の発明と同様な効果を奏する。

【0050】次に、請求項16に対応する発明は、請求項1、2又は3記載の電子文書の改竄防止システムにて生成された認証データから第2の暗号化データを取出

し、これを第2の秘密鍵に対応する第2の公開鍵で復号化する第2の復号化ステップと、第2の復号化ステップにより復号化されたデータから第1の暗号化データを取出し、これを第1の秘密鍵に対応する第1の公開鍵で復号化する第1の復号化ステップと、電子文書から特徴を抽出して照合用特徴データを生成する特徴抽出ステップと、第1の復号化ステップにより復号化されたデータから特徴データを取出し、これを照合用特徴データと照合する照合ステップと、照合ステップによる照合結果と、第2の復号化手段により復号化されたデータから取り出された外部認証データによって、外部認証者による認証の事実及び認証の日付を出力するステップとを有する認証文書確認方法である。

【0051】本発明はこのような手段を設けたので、請求項5の発明と同様な効果を奏する。

【0052】次に、請求項17に対応する発明は、請求項1の発明を実現させるためのプログラムを格納した記録媒体についての発明であり、このプログラムを実行する計算機は、請求項1の発明における第2の暗号化手段を除いたものと同様な作用効果を奏する。

【0053】次に、請求項18に対応する発明は、請求項1、2又は3記載の電子文書の改竄防止システムにて生成された認証データから第2の暗号化データを取出し、これを第2の秘密鍵に対応する第2の公開鍵で復号化する第2の復号化手段と、第2の復号化手段により復号化されたデータから第1の暗号化データを取出し、これを第1の秘密鍵に対応する第1の公開鍵で復号化する第1の復号化手段と、電子文書から特徴を抽出して照合用特徴データを生成する特徴抽出手段と、第1の復号化手段により復号化されたデータから特徴データを取出し、これを照合用特徴データと照合する照合手段と、照合手段による照合結果と、第2の復号化手段により復号化されたデータから取り出された外部認証データによって、外部認証者による認証の事実及び認証の日付を出力する手段として、コンピュータを機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体である。

【0054】本発明はこのような手段を設けたので、このプログラムを実行する計算機は、請求項5の発明と同様な作用効果を奏する。

【0055】次に、請求項19に対応する発明は、請求項1の発明における処理が実行された結果として得られるデータ構造が記録された記録媒体についての発明である。

【0056】次に、請求項20に対応する発明は、請求項3の発明における処理が実行された結果として得られるデータ構造が記録された記録媒体についての発明である。

【0057】次に、請求項21に対応する発明は、認証付き電子文書から電子文書を取り出して、これに変更を

加えて、新たな電子文書を生成する文書変更手段と、認証付き電子文書から取り出された元の電子文書と新たな電子文書との変更点を抽出して変更箇所データを取得する差分抽出手段と、変更箇所データと新たな電子文書とをそれぞれ変更者認証する変更者認証手段と、変更者認証手段により認証された各データを外部の認証システムに送出するとともに、それぞれを外部認証された認証データを受け取って、受け取った各認証データ及び新たな電子文書に基づいて、認証付き変更箇所データと新たな認証付き電子文書を生成する認証手段とを備えた電子文書の改竄防止システムである。

【0058】本発明はこのような手段を設けたので、変更された電子文書に新たな認証を付することができるのと同時に、変更部分のみのデータも認証することができ、変更電子文書の改竄を防止できる。また、外部認証を得ているので信頼性も高い。

【0059】次に、請求項22に対応する発明は、請求項21に対応する発明において、変更者認証手段は、変更箇所データ及び又は新たな電子文書から特徴抽出して特徴データを出力する特徴抽出手段と、特徴データを、新たな電子文書を生成した変更者の暗号化鍵で暗号化して出力する暗号化手段とを備えた電子文書の改竄防止システムである。

【0060】本発明はこのような手段を設けたので、変更箇所データ及び又は新たな電子文書そのものでなく、その特徴データを暗号化したものを認証データとするために認証元の特徴を残しつつ安全性を高めることができる。さらに認証データのデータ量を少なくできる。

【0061】次に、請求項23に対応する発明は、請求項22に対応する発明において、変更者認証手段は、暗号化手段から出力されかつ新たな電子文書に対応する暗号化特徴データと、元の認証付き電子文書から取り出された以前の認証データとを結合して出力する結合手段を備えた電子文書の改竄防止システムである。

【0062】本発明はこのような手段を設けたので、変更後の新たな電子文書に付する認証データに以前の認証データを含めることができ、変更毎の履歴とすることができる。また、各回の認証データを保持できる。

【0063】次に、請求項24に対応する発明は、請求項22に対応する発明において、変更者認証手段は、特徴抽出手段により特徴抽出された特徴データと、元の認証付き電子文書から取り出された以前の認証データとを結合して出力する結合手段を備え、暗号化手段の暗号化対象として、結合手段からの出力データの特徴データに代えて入力する電子文書の改竄防止システムである。

【0064】本発明はこのような手段を設けたので、請求項23に対応する発明と同様な効果を他の手法で実現できる。

【0065】次に、請求項25に対応する発明は、請求項21乃至24のうち何れか1項に記載された認証手段

により生成された認証付き変更箇所データと認証付き電子文書とを含む変更済電子文書から、認証付き変更箇所データ及び認証付き電子文書を取り出す分離手段と、請求項21乃至24のうち何れか1項に記載された文書変更手段、差分抽出手段、変更者認証手段及び認証手段と、認証手段により生成された新たな認証付き変更箇所データ及び新たな認証付き電子文書と、分離手段で分離された元の認証付き変更箇所データとに基づき、新たな変更済電子文書を生成する結合手段とを備えた電子文書の改竄防止システムである。

【0066】本発明はこのような手段を設けたので、複数回の変更があっても変更後の電子文書を増やすことなく、かつ各変更毎の認証データを保持できる変更済電子文書を作成することができる。

【0067】次に、請求項26に対応する発明は、請求項21乃至24のうち何れか1項に記載された変更者認証手段により認証された各データを受け取る受入手段と、各データそれぞれに、少なくとも日付データ及び認証実行識別情報を結合する結合手段と、この結合手段により結合された各データを外部認証機関の暗号鍵によって暗号化して、外部認証された認証データを作成する暗号化手段とを備えた電子文書の外部認証システムである。

【0068】本発明はこのような手段を設けたので、変更電子文書の確実かつ安全な認証を行うことができる。

【0069】次に、請求項27に対応する発明は、請求項26に記載の外部認証システムにより外部認証された認証データを、外部認証機関の復号鍵で復号する復号化手段と、復号化手段により復号された認証データから、日付データ及び認証実行識別情報を取り出すデータ取出手段とを備えた認証文書確認システムである。

【0070】本発明はこのような手段を設けたので、認証日付及び外部認証機関における認証情報（認証実行ID等）を取得することができる。

【0071】次に、請求項28に対応する発明は、請求項27に対応する発明において、請求項26に記載の外部認証システムにより外部認証された認証データが請求項23に対応しかつ電子文書に対応するものである場合に、復号化手段により復号された認証データから、以前の認証データを取り出す認証データ取出手段を備えた認証文書確認システムである。

【0072】本発明はこのような手段を設けたので、複数回の変更認証がなされている場合、各回の認証データひいては外部認証情報を取り出すことができる。

【0073】次に、請求項29に対応する発明は、請求項28に対応する発明において、復号化手段により復号された認証データのうち、請求項22の暗号化手段で暗号化された暗号データが入力されるとともに、当該暗号データを変更者の復号鍵で復号して特徴データを取り出す第2の復号化手段と、請求項21の文書変更手段で得

10

20

30

40

50

られた新たな電子文書から特徴抽出して比較用特徴データを出力する特徴抽出手段と、第2の復号化手段で得られた特徴データと、特徴抽出手段で得られた比較用特徴データとを比較する照合手段とを備えた認証文書確認システムである。

【0074】本発明はこのような手段を設けたので、電子文書が真正なものであるかを確認することができる。

【0075】次に、請求項30に対応する発明は、請求項27に対応する発明において、請求項26に記載の外部認証システムにより外部認証された認証データが請求項24に対応しかつ電子文書に対応するものである場合に、復号化手段により復号された認証データを変更者の復号鍵で復号する第2の復号化手段と、第2の復号化手段で復号化された認証データから、以前の認証データを取り出す認証データ取出手段とを備えた認証文書確認システムである。

【0076】本発明はこのような手段を設けたので、請求項28に対応する発明と同様な効果を他の手法で得ることができる。

【0077】次に、請求項31に対応する発明は、請求項30に対応する発明において、第2の復号化手段で復号化された認証データから、特徴データを取り出す分離手段と、請求項21の文書変更手段で得られた新たな電子文書から特徴抽出して比較用特徴データを出力する特徴抽出手段と、分離手段で得られた特徴データと、特徴抽出手段で得られた比較用特徴データとを比較する照合手段とを備えた認証文書確認システムである。

【0078】本発明はこのような手段を設けたので、請求項29に対応する発明と同様な効果を他の手法で得ることができる。

【0079】次に、請求項32に対応する発明は、請求項27に対応する発明において、請求項26に記載の外部認証システムにより外部認証された認証データが請求項22に対応しかつ変更箇所データに対応するものである場合に、復号化された認証データのうち、請求項22の暗号化手段で暗号化された暗号データが入力されるとともに、当該暗号データを変更者の復号鍵で復号して特徴データを取り出す第2の復号化手段と、請求項21の差分抽出手段で得られた変更箇所データから特徴抽出して比較用特徴データを出力する特徴抽出手段と、第2の復号化手段で得られた特徴データと、特徴抽出手段で得られた比較用特徴データとを比較する照合手段とを備えた認証文書確認システムである。

【0080】本発明はこのような手段を設けたので、各回における変更箇所データの正当性が確認でき、ひいては電子文書が真正なものであるかを確認できる。

【0081】次に、請求項33に対応する発明は、請求項25に記載された電子文書の改竄防止システムにより作成された変更済電子文書の変更部分についての認証確認を行うシステムであって、請求項28又は30の認証

文書確認システムと、請求項32の認証文書確認システムとを備えるとともに、複数回の変更を受けた最終的な変更済電子文書における認証付き電子文書から、最終変更回に関する認証データを取り出し、まずこれを請求項26に記載の外部認証システムにより外部認証された認証データとして請求項28又は30の認証文書確認システムに入力し、最終変更回以外の各回については、請求項28又は30の認証文書確認システムから出力される以前の認証データを、請求項26に記載の外部認証システムにより外部認証された認証データとして、順次、請求項28又は30の認証文書確認システムに入力し、また、複数回の変更を受けた最終的な変更済電子文書から、各回の認証付き変更箇所データを取り出し、この認証付き変更箇所データを変更箇所データ及び請求項26に記載の外部認証システムにより外部認証された認証データに分離して、請求項32の認証文書確認システムに入力し、請求項28又は30の認証文書確認システムから得られた日付データ及び認証実行識別情報と、請求項32の認証文書確認システムから得られた日付データ及び認証実行識別情報とを各変更回毎に照合する変更済電子文書の認証確認システムである。

【0082】本発明はこのような手段を設けたので、変更済電子文書の真実性を確認でき、証拠としての使用を可能とする。

【0083】次に、請求項34に対応する発明は、請求項33に対応する発明において、請求項29又は31の認証文書確認システムを備えるとともに、最終的な変更済電子文書に包含される認証付き電子文書から取り出された認証データ及び新たな電子文書を、請求項28又は30の認証文書確認システムに代えて請求項29又は31の認証文書確認システムに入力する変更済電子文書の認証確認システムである。

【0084】本発明はこのような手段を設けたので、より一層電子文書の証拠能力を高めることができる。

【0085】次に、請求項35に対応する発明は、請求項21に対応する発明をコンピュータに実現させるプログラムを記録した記録媒体である。

【0086】この記録媒体から読み出されたプログラムにより制御されるコンピュータは、請求項21の電子文書の改竄防止システムとして機能する。

【0087】次に、請求項36に対応する発明は、請求項22に対応する発明をコンピュータに実現させるプログラムを記録した記録媒体である。

【0088】この記録媒体から読み出されたプログラムにより制御されるコンピュータは、請求項22の電子文書の改竄防止システムとして機能する。

【0089】次に、請求項37に対応する発明は、請求項27に対応する発明をコンピュータに実現させるプログラムを記録した記録媒体である。

【0090】この記録媒体から読み出されたプログラム

により制御されるコンピュータは、請求項27の認証文書確認システム電子文書の改竄防止システムとして機能する。

【0091】

【発明の実施の形態】次に、本発明の実施の形態について説明する。

【0092】[第1～第13の実施形態についての説明] 図1は本発明の各実施形態における電子文書の改竄防止システム及び方法の全体的な構成を示す図である。

【0093】公衆回線や専用回線を用いたネットワーク100が構成され、当該ネットワークに文書認証システム101や外部認証機関99の外部認証システム102、認証文書確認システム103が接続されている。

【0094】文書認証システム101は、認証対象となる電子文書に関する当該システム使用者作成の所定情報（使用者の鍵で暗号化したことによる一種の使用者認証を含む）をネットワーク100を介して外部認証システム102に送付し、この所定情報を元に外部認証システム102で作成された認証のための情報の返信を受け認証電子文書を作成する。また、後の実施形態でも説明するが、複数の文書認証システム101でそれぞれ異なるシステム使用者に加工（暗号化や認証情報付加等であり、各使用者による実質的な認証になっている）された所定情報が外部認証システム102に送付される場合もある。

【0095】一方、認証文書確認システム103は、上記認証電子文書の正当性を確認するためのシステムであり、ネットワーク100を介し文書認証システム101等から確認対象の認証電子文書を受信する。

【0096】文書認証システム101、外部認証システム102及び認証文書確認システム103は、ワークステーションやパーソナルコンピュータ等の計算機に表示装置、入力装置、あるいは例えば指紋読取り機等を付加したものであり、基本的にはその動作プログラムが相違することで異なる各機能を実現する。したがって、図1に示すように、例えば文書認証システム101と認証文書確認システム103とが同一の計算機上に構成される場合もある。

【0097】さらに、文書認証システム101と外部認証システム102とを同一計算機、あるいはLAN等で接続される計算機上に構成させ、外部認証機関において認証作業のすべてを行うようにすることも可能である。

【0098】本発明にかかわる電子文書の改竄防止システム及び方法は、これらの文書認証システム101、外部認証システム102及び認証文書確認システム103を適宜組み合わせ、あるいはその一部機能を適宜組み合わせてなるものである。

【0099】また、上記場合は、ネットワークを介した情報の瞬時転送を前提とした場合を説明しているが、図1に示すように、フロッピーディスク等の記録媒体9

7、98を介して文書認証システム101～外部認証システム102間、あるいは文書認証システム101～認証文書確認システム103間で必要情報（所定情報や電子文書）の交換を行うことも可能である。

【0100】全体的には以上のシステム構成を有する電子文書の改竄防止システム及び方法について、その各実施形態を以下に説明する。

【0101】（第1の実施の形態）本実施形態は改竄を防止できる電子文書の作成システム及び方法に関するものである。

【0102】図2は本発明の第1の実施の形態に係る電子文書の改竄防止システムに適用される文書認証システムのハードウェア構成例を示すブロック図である。

【0103】文書認証システムは、計算機110に、表示装置111、入力装置112、印刷装置113、外部記憶装置114、指紋読取り機64、スキャナ115が接続されてなっている。

【0104】計算機110においては、CPUバス116にCPU117、ROM118、RAM119が接続され、さらに、CPUバス116に接続される各インターフェース手段120、121、122、123、124、125、126、127を介してそれぞれハードディスク装置128、通信装置121、表示装置111、入力装置112、印刷装置113、外部記憶装置114、指紋読取り機64、スキャナ115が接続されている。

【0105】ROM118は、コンピュータ110を起動しオペレーティングシステム（OS）等を立ち上げるのに用いられるブート処理プログラム等が格納されている。

【0106】また、ハードディスク装置128には、プログラム格納部130及びデータ格納部131が設けられている。プログラム格納部130は、OSや、文書認証システム101を実現するプログラム等を格納し、データ格納部131は、電子文書、認証付き電子文書、その他各種情報を格納する。

【0107】RAM119は、いわゆる主記憶に使用される。すなわち、CPU117による各種処理のための作業領域132を備え、またCPU117を制御する文書認証プログラム133を格納している。

【0108】この文書認証プログラム133は、ハードディスク装置128のプログラム格納部130から呼び出され、RAM119内に格納されるものである。

【0109】CPU117は、RAM119内の文書認証プログラム133に従って各部を制御し、文書認証システム101を実現する。つまり、RAM119（特に文書認証プログラム133）やハードディスク装置128等のソフトウェア資源とCPU117等の図2のハードウェア資源とが結合して文書認証システム101の各機能実現手段が構成される。本実施形態及び以下の各実

施形態における処理説明図や流れ図等に表現される各手段（各処理）あるいは図示しない各手段（各処理）は、このような機能実現手段であり、主として文書認証プログラム133に従うCPU117の動作によるものである。

【0110】通信装置129は、外部認証システム102と間あるいは認証文書確認システム103と間の通信を行うものである。電子文書や各種情報の授受が行われる。

【0111】外部記憶装置114は、電子文書、認証付き電子文書、その他各種情報を可搬な記録媒体に格納し、特に認証付き電子文書の保存、送付等を便利かつ容易にするものである。外部記憶装置114としては、例えばフロッピーディスク装置、光磁気ディスク装置（MO）、CD-R、CD-R/WあるいはDVD等が用いられる。

【0112】指紋読取り機64は、人間の指紋情報を読み取る装置である。システム使用者の認証や暗号情報作成等のために用いられる。

【0113】スキャナ115は、印鑑等の図形をイメージ情報として読み取る装置である。

【0114】次に外部認証システムのハードウェア構成について説明する。

【0115】図3は本実施形態の電子文書の改竄防止システムに適用される外部認証システムのハードウェア構成例を示すブロック図であり、図2と同一部分には同一符号を付してその説明を省略する。

【0116】外部認証システム102は、文書認証システム101と同様な計算機システムから構成される。文書認証システム101との相違点は、ハードディスク装置128のプログラム格納部130に格納される動作プログラムである。この動作プログラムが呼び出され、RAM119内に外部認証プログラム134として格納される。CPU117は、この外部認証プログラム134に従って各部を制御し、外部認証システム102が実現される。また、ソフトウェア資源（特に外部認証プログラム134）とハードウェア資源とが結合して機能実現手段が構成される点も文書認証システム101の場合と同様である。

【0117】次に、図4を用いて電子文書の改竄防止システムの各機能について説明する。図4は本実施形態の電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図である。

【0118】この電子文書の改竄防止システムは、文書認証システム101と外部認証システム102とから構成されている。

【0119】文書認証システム101は、認証すべき電子文書1から特徴データ3Dを抽出し暗号化するとともに、この暗号化データ6について認証を与える外部認証機関の外部認証システム102から合成データ10を受

け取り、これを上記電子文書1に付与して認証付き電子文書12を作成する。

【0120】このために文書認証システム101は、見出し3Hの取出編集手段（図示せず）と、電子文書1から特徴抽出を行って特徴データ3Dを生成する特徴抽出手段2と、特徴データ3Dを第1の秘密鍵4（#1）

（以下、複数存在し得る同種類の構成やデータには、場合により#1、#2、...あるいは第1の、第2の、...と記して区別する）にて暗号化し暗号化データ6D（#1）を生成する暗号化手段6と、見出し3Hと暗号化データ6Dとを結合する手段（図示せず）と、結合された見出し付き暗号化データ6を外部認証システム102に送信する通信手段（図示せず）と、外部認証システム102から受け取った合成データ11を電子文書1に付与して認証付き電子文書12を作成し電子媒体に保存する手段（図示せず）を備えている。

【0121】一方、外部認証システム102は、文書認証システム101から受け取った見出し付き暗号データ6を分離手段（図示せず）で分離し、このうちの暗号データ7Dに外部認証データ7A（#1）を付与しこれを暗号化手段9を用いて第2の秘密鍵8（#2）にて暗号化した後、この暗号データ10Dと見出し10Hからなる合成データ10を結合手段（図示せず）で結合して通信手段（図示せず）により文書認証システム101に送信する。

【0122】なお、本実施形態では、各データの暗号化方式として秘密鍵と公開鍵を使用したRSA方式が用いられるが、他の暗号化方式（DES方式等）を用いてもよい。

【0123】次に、以上のように構成された本発明の実施の形態に係る電子文書の改竄防止システムの動作について図4及び図5を用いて説明する。

【0124】図5は本実施形態の電子文書の改竄防止システムの動作を示す流れ図である。

【0125】まず、文書認証システム101において電子文書1のデータが読み込まれ（S1）、その文書データから文書タイトルや日付等の見出し3Hのデータに使用できる部分が取り出され、更に補足説明を追加する為に編集が行われる。こうして見出し3が作成される（S2）。なお、見出し3には例えば第7実施形態で説明する文書作成者の電子印鑑や電子署名等も含まれる。

【0126】次に、特徴抽出手段2により電子文書1から特徴が抽出され特徴データ3Dが作成される（S3）。ここで、特徴データ3Dは、例えば電子文書の1ビットが変化しても異なった値となるような電子文書自体の特徴を示すデータである。一方、見出し3Hは特徴データ3Dがどの電子文書のものであるかを分かるようにする為に追加されるデータである。見出し3Hと特徴データ3Dは合成データ（見出し付き特徴データ3）として対応が取られるようにする。

10

20

30

40

50

【0127】次に、暗号化手段5により秘密鍵4（#1）が用いられ、特徴データ3Dが暗号化され第1の暗号データ6Dが生成される（S4）。なお、第1の秘密鍵4は電子文書1の作成者が保有する秘密鍵であり、他人には知らせないようにしたものである。

【0128】次に、見出し6Hと暗号データ6Dを結合し見出し付き暗号データ6として対応が取られる（S5）。なお、見出し6Hは見出し3Hと同じものである。このようにしてできた見出し付き暗号データ6は外部認証機関の外部認証システム102に送信される（S6）。なお、この送信は、本実施形態では公衆回線や専用回線を介し、ネットワーク100に伝送されるが、例えばフロッピーディスク等の電子媒体に記録して郵送等してもよい。

【0129】一方、外部認証機関では、文書認証システム101からの見出し付き暗号データ6が受信される（S7）。

【0130】外部認証システム102では見出し付き暗号データ6が見出し7Hと暗号データ7Dに分解される（S8）。このうちの暗号データ7Dに外部認証データ7Aが結合される（S9）。この外部認証データ7Aは、文書認証システム101が認証を要求してきたデータについて第三者である外部認証機関が認証したことを示す情報であり、認証した日付データが含まれる。

【0131】次に、暗号化手段9により第1の暗号データ7D（#1）と外部認証データ7A（#1）が纏められ、秘密鍵8で暗号化される（S10）。こうして第2の暗号データ10D#2が生成される。これにより第2の暗号データ10D（#2）は作成者の秘密鍵4と外部認証機関の秘密鍵8で二重に鍵が掛けられたデータとなり、かつそれぞれ独自のデータが含まれる。

【0132】さらに、第2の暗号データ10Dは見出し10Hと合成されて合成データ10となり、その取り扱いが容易に形になる（S11）。なお、見出し10Hは見出し3Hと同じ内容である。そして、合成データ10は外部認証システム102から第三者認証を要求する作成者の文書認証システム101にネットワーク100を介して返信される（S12）。

【0133】文書認証システム101では、合成データ10が合成データ11として受け取られる（S13）。そして、この合成データ11は電子文書1と合成されて認証付き電子文書12が生成される。このような結合をすればデータ取り扱いが容易になる。生成された認証付き電子文書12は任意の場所の電子媒体に保管することができ、何れの場所に保管されても認証機能を発揮することになる。なお、ここでいう結合というのは、単に同一の記録媒体に合成データ11と電子文書1とを記録する場合や、両者の関連付けを示す他のデータを作成する場合等、様々な場合を含むものである。この結合する手段は、請求項における電子文書の認証データとする手段

の一例でもある。

【0134】上述したように、本発明の実施の形態に係る電子文書の改竄防止システム及び方法は、本人により電子署名された文書を外部認証機関が認証する手順を踏むことにより、外部認証機関の認証日付にはまさしく本人が文書を作成していたことが証明される。また、たとえ電子署名がない場合であっても、文書作成者本人の秘密鍵4で特徴データの暗号化がなされ、これに対応する公開鍵で復号化されることになるので、何れにしても文書作成者の作成になる文書であることが認証される。

【0135】また、文書本体の改竄を行うと改竄後の文書から抽出されるべき特徴データが変化し、先に認証用に抽出された特徴データ3Dと異なるものになることによって元文書の改竄の事実が検出できる。一方、先に認証用に抽出された特徴データ3Dは、外部認証機関の認証データ7Aと共に認証機関の秘密鍵8で暗号化されているので、認証付き電子文書12に付されている暗号データ11Dの改竄は不可能である。したがって、たとえ本人であっても外部認証後には文書改竄が不可能になる。

【0136】これにより裁判の場で文書の正当性が証明できる、証拠能力のある電子文書が生成でき、従来紙で保存していた重要文書や、証拠書類を電子化する事が可能となる。また、従来の紙の文書でも改竄の有無を判定するには高度な技術が必要とされたが、本発明になる電子文書の改竄防止システムでは電子的な手順を踏むだけで改竄の有無を確認できるので、改竄の有無を容易に証明できる。さらに電子化により保管場所が削減されると共に、遠隔地への文書電送が瞬時に行えるようになり、コンピュータによる検索が行えるようになる。こうして、商取引の信用向上、取引の迅速化を図ることができる。

【0137】また、本実施形態の文書改竄防止システムでは、文書認証システム101や外部認証システム102においてそれぞれ電送データの暗号化が行われるので、ネットワーク100として公衆回線を用いても安全である。

【0138】さらに、外部認証機関が認証した外部認証データを元の電子文書に結合して認証付き電子文書12の形で管理するようにしたので、電子文書を保存する時の扱いが楽になる。

【0139】（第2の実施の形態）本実施形態では第1の実施形態で認証した認証付き電子文書12が真正なものであることを確認し、また外部認証機関の付した認証日付等の認証情報を取り出すシステムについて説明する。

【0140】この電子文書の改竄防止システムは、図1に示した認証文書確認システム103として構成されるものである。

【0141】図6は本発明の第2の実施の形態に係る電

子文書の改竄防止システムに適用される認証文書確認システムのハードウェア構成例を示すブロック図であり、図2と同一部分には同一符号を付してその説明を省略する。

【0142】認証文書確認システム103は、文書認証システム101と同様な計算機システムから構成される。文書認証システム101との相違点は、ハードディスク装置128のプログラム格納部130に格納される動作プログラムである。この動作プログラムが呼び出され、RAM119内に認証文書確認プログラム135として格納される。CPU117は、この認証文書確認プログラム135に従って各部を制御し、認証文書確認システム103が実現される。また、ソフトウェア資源（特に認証文書確認プログラム135）とハードウェア資源とが結合して機能実現手段が構成される点も文書認証システム101の場合と同様である。

【0143】次に、図7を用いて電子文書の改竄防止システムの各機能について説明する。図7は本実施形態の電子文書の改竄防止システムに適用される認証文書確認システム103の機能構成及び処理流れの一例を示す図であり、図4と同一部分には同一符号を付して説明を省略する。

【0144】この認証文書確認システム103は、認証付き電子文書12から取り出した特徴データ18Dと認証付き電子文書12から合成データ11を取り除いた電子文書19から抽出される特徴データ21とを照合し、電子文書の同一性を行うとともに、認証データ（暗号データ11D）より取り出された外部認証データ15Aから外部認証機関99による認証の事実及びその認証日付を確認する。

【0145】このために認証文書確認システム103には、外部記憶装置114やハードディスク装置128に格納された認証付き電子文書12から見出し11H及び暗号データ11Dを取り出す手段（図示せず）と、暗号データ11Dを外部認証システム102の第2の公開鍵13（#2）により復号化する復号化手段14と、この復号化により得られたデータのうちの外部認証データ15A（#1）により日付認証15A-D及び外部認証機関99の認証確認を行う手段（図示せず）と、復号化手段14で復号化されたデータのうちの暗号データ15Dを文書認証システム101の第1の公開鍵16（#1）で復号化する復号化手段17とが設けられている。さらに、認証データを取り除いた電子文書19から特徴データ21を取り出す特徴抽出手段20と、この特徴データ21と、復号化手段17で復号化された見出し付き特徴データ18から取り出した特徴データ18Dとを照合し、電子文書19が電子文書1と同一であるか否かの同一性判定22-Jを行う照合手段とが設けられている。

【0146】本実施形態では、秘密鍵と公開鍵を使用した暗号としてはRSA方法が用いられるが、他の暗号化

方式（DES方式等）を用いてもよい。なお、図7に示す認証文書確認システム103は電子文書1の作成者のシステムでも第三者のシステムでもかまわない。

【0147】次に、以上のように構成された本発明の実施の形態に係る電子文書の改竄防止システムの動作について図7及び図8を用いて説明する。

【0148】図8は本実施形態の電子文書の改竄防止システムの動作を示す流れ図である。

【0149】まず、外部記憶装置114、ハードディスク装置128から、あるいはネットワーク100を介して電子文書12が読み込まれ（T1）、合成データ11が取り出される（T2）。

【0150】合成データ11の中から更に認証データとして機能する第2の暗号データ11D（#2）が取り出される（T3）。第2の公開鍵13（#2）を使用して復号化手段14で復号が行われる（T4）。なお、第2の公開鍵13（#2）は外部認証機関99の公開鍵であり、第2の秘密鍵8（#2）に対応するものである。これによって第1の暗号データ15D（#1）と外部認証データ15A（#1）とが取り出される。

【0151】次に、見出し付き認証データ15から暗号データ15Dと外部認証データ15Aとが分離される（T5）。なお、暗号データ15Dは図4の暗号データ6Dと内容が同一のものである。また、外部認証データ15Aは図4の外部認証データ7Aと内容が同一のものである。さらに、見出しデータ15Hは図4の見出しデータ3Hと内容が同一のものである。

【0152】次に、復号された外部認証データ15Aから日付認証データ15A-Dが取り出され、外部認証機関が合成データ6の認証を行った日付が確認される（T6）。

【0153】一方、第1の暗号データ15D（#1）は第1の公開鍵16（#1）で復号化手段17によって復号され（T6）、第1の特徴データ18Dが生成される。第1の公開鍵16（#1）は電子文書の作成者の公開鍵であり、第1の秘密鍵4（#1）に対応するものである。なお、特徴データ18Dは第1の特徴データ3D（#1）と内容が同一のものである。

【0154】次に、電子文書12から合成データ11を除いた電子文書19が取り出される（T8）。この電子文書19は元の電子文書1に対応するものである。さらに、電子文書19から特徴抽出手段20により特徴データ21が取り出される（T9）。特徴抽出手段20は特徴抽出手段2と同一の手段であり、電子文書19の内容が電子文書1と同一であれば同一の特徴データが生成される。

【0155】次に、特徴データ18Dと特徴データ21とが照合手段22により照合され（T10）、照合結果が同一かどうかを示す同一性判定結果22-Jが出力される。同一性判定結果22-Jが判定良（一致）であれ

ば(T11)、日付認証データ15A-Dの日付で認証された本人作成の文書である事が証明される。そこで、ステップT6で取り出した日付認証と共に文書同一である旨が表示装置111に表示される(T13)。

【0156】一方、同一性判定結果22-Jが判定不良（不一致）であれば（T11）、不一致が表示される。

【０１５７】上述したように、本発明の実施の形態に係る電子文書の改竄防止システム及び方法は、暗号化特徴データの付加、本人電子署名及び外部認証機関の認証がなされた電子文書から外部認証機関の外部認証データを取り出し、また付加されている特徴データと電子文書本体からの特徴データとを文書作成者の公開鍵１６を用いて照合することで、外部認証機関の認証日付にはまさしく本人が文書を作成していたことが証明される。

【0158】電子文書本体の改竄を行うと、電子文書19から抽出される特徴データ21が変化することにより、一方、第1の特徴データ3D、18Dは外部認証機関99によって改竄を防止される事によって、本人であっても外部認証後には文書改竄が不可能になる。これにより裁判の場で文書の正当性が証明でき、従来紙で保存していた重要文書や、証拠書類を電子化する事が可能となる。

【0159】また、従来の紙の文書でも改竄の有無を判定するには高度な技術が必要とされたが、上記照合処理により電子文書の改竄防止システムでは容易に改竄の有無を証明できる。さらに、電子化により保管場所が削減されると共にネットワークを介して遠隔地への電送が瞬時に行い得る。したがって、さらに、コンピュータによる検索も可能である。

【０１６０】また、本実施形態の文書改竄防止システムでは、文書認証システム１０１や外部認証システム１０２においてそれぞれ電送データの暗号化が行われるので、ネットワーク１００として公衆回線を用いても安全である。

【0161】さらに、外部認証機関が認証した認証データを元の電子文書に結合する事により、文書を保存する時の扱いが楽になる。

【０１６２】（第３の実施の形態）本実施形態の電子文書の改竄防止システム及び方法では、一旦作成された認証付き電子文書１２に付された合成データ１１にさらに外部認証データを付し、暗号化をかけ直す。これにより改竄防止を強化した電子文書を生成し、認証付き電子文書１２の作成から長期間を経た認証データの秘匿性を維持するものである。

【０１６３】図９は本発明の第３の実施の形態の電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図であり、図４及び図７と同一部分には同一符号を付し、その説明を省略する。また、本実施形態のシステムには、図２及び図３に示す文書認証システム１０１及び外部認証システム１０２が用いられており、本実施形

態の独自の機能部分は、文書認証プログラム 133 あるいは外部認証プログラム 134 に修正が加えられたことによるものである。

【0164】この電子文書の改竄防止システムは、図1に示す文書認証システム101と外部認証システム102とから構成されている。

【0165】文書認証システム101は、電子文書12から合成データ11を取出し、外部認証システム102に送付する手段(図示せず)と、電子文書12から認証データ11を取り除いて元の電子文書としたものに外部認証システム102から受け取った見出し付き暗号データ27を認証データとして付加して認証付き電子文書28とする手段(図示せず)とが加えられる他、第1の実施形態と同様に構成されている。

【 0 1 6 6 】一方、外部認証システム 1 0 2 は、文書認証システム 1 0 1 からの合成データ 1 1 に外部認証データ 2 3 A を付加するとともに、暗号データ 2 3 D (暗号データ 1 1 D と同一) と外部認証データ 2 3 A とを第 3 の秘密鍵 2 4 (# 3) で暗号化する暗号化手段 2 5 と、この暗号化された暗号データ 2 6 D と見出し 2 6 H からなる見出し付き暗号データ 2 6 を文書認証システム 1 0 1 に送信する手段 (図示せず) とが加えられる他、第 1 の実施形態と同様に構成されている。なお、第 3 の秘密鍵 2 4 (# 3) は、外部認証機関 9 9 のもう一つの秘密鍵である。

【０１６７】次に、以上のように構成された本発明の実施の形態に係る電子文書の改竄防止システムの動作について図９及び図１０を用いて説明する。

【0168】図10は本実施形態の電子文書の改竄防止システムの動作を示す流れ図である。

【0169】まず、文書認証システム101において、外部記憶装置114、ハードディスク装置128から、あるいはネットワーク100を介して電子文書12が読み込まれ（U1）、認証データである合成データ11が取り出される（U2）。この合成データ11が外部認証機関99の外部認証システム102にネットワーク100を介して送信される（U3）。

$$[0170])$$

【0171】次に、外部認証システム102において、ステップU3で送信された合成データ11（認証データ）が受信される。次に受け取った合成データ11が見出し23Dと暗号データ23Dに分離される（U5）。ここで見出し付き認証データ23に外部認証データ23Aが追加される。なお、外部認証データ23Aは、第1の実施形態の外部認証データ7Aと同様なものであり、認証日等の情報が含まれる。

【0172】次に、暗号データ23Dと外部認証データ23Aが結合され(U6)、この結合データが秘密鍵24(＃3)にて暗号化され暗号データ26Dが生成される(U7)。なお、この秘密鍵24は、外部認証機関9

9の秘密鍵であり、例えばRSA方式に対応するものである。

【0173】次に、見出し26Hと暗号データ26Dとが結合されてなる認証データである暗号データ26が生成され(U8)、当該データ26が文書認証システム101にネットワーク100を介して送信される(U9)。

【0174】外部認証機関99から送信された暗号データ26が文書認証システム101により受信される(U10)。これが見出し付き暗号データ27とされ、電子文書12から暗号データ11を取り除いた元の電子文書に合成されて認証付き電子文書28が生成される(U11)。こうして改竄防止が強化された電子文書が生成されることになる。なお、電子文書28は外部記憶装置114やハードディスク装置128、その他の任意の場所の電子媒体に保管することができる。

【0175】上述したように、本発明の実施の形態に係る電子文書の改竄防止システム及び方法は、電子文書12から取り出した合成データ11に再度外部認証機関99の認証を与え、暗号をかけ直して認証付き電子文書28を生成するようにしたので、改竄防止を強化した文書28を作成することができる。

【0176】したがって、暗号技術の進歩により、最初の暗号が解読される恐れがある年数を経過する前に、更に新しい暗号により文書1の改竄防止を強化することでき、たとえ長期間の電子文書保管を行っても、裁判の場で文書の正当性が証明できるようになる。

【0177】なお、本実施形態では、電子文書12の如く1度の認証の電子文書を再認証する場合を説明したが、本実施形態の手法を用いて電子文書28をさらに再認証するようにしてもよい。このように再認証を繰り返して認証の回数を重ねる事によって、電子文書1の保管年限が延長でき、事実上無限長とすることができる。したがって、本実施形態では、公開鍵方式(RSA)の暗号方式で際認証する場合を説明したが、その時々に関発された最も解読困難な暗号方式で適宜再認証(再暗号化)することが適当である。

【0178】(第4の実施の形態)本実施形態では第3の実施形態で再認証し改竄防止を強化した認証付き電子文書28が真正なものであることを確認し、また外部認証機関の付した各認証日付等の認証情報を取り出すシステムについて説明する。

【0179】図11は本発明の第4の実施の形態の電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図であり、図4、図7及び図9と同一部分には同一符号を付し、その説明を省略する。また、本実施形態のシステムには、図6に示す認証文書確認システム103が用いられており、本実施形態の独自の機能部分は、認証文書確認プログラム135に修正が加えられたことによるものである。

【0180】この電子文書の改竄防止システムは、図1に示した認証文書確認システム103として構成されるものである。

【0181】認証文書確認システム103は、認証付き電子文書28から取り出した認証データについて3回の復号処理を施して特徴データ18Dを取出し、電子文書19から取り出した特徴データ21との照合を行うとともに、その過程で、外部認証機関99による2回の認証についてそれぞれの認証日付及び外部認証の旨の確認を行うようになっている。

【0182】このために、認証文書確認システム103には、認証付き電子文書28から見出し付き暗号データ27を取り出す手段(図示せず)と、外部認証機関99の公開鍵29(#3)により暗号データ27Dを復号化する復号化手段30と、復号化された外部認証データ31Aから外部認証機関99の認証確認を行い日付認証31A-Dを取り出す手段(図示せず)とが設けられる。他、図7に示す第2の実施形態と同様に構成されている。なお、復号化手段14が復号するデータは、暗号データ31Dである。

【0183】次に、以上のように構成された本発明の実施の形態に係る電子文書の改竄防止システムの動作について図11及び図12を用いて説明する。

【0184】図12は本実施形態の電子文書の改竄防止システムの動作を示す流れ図である。

【0185】まず、認証文書確認システム103において、外部記憶装置114、ハードディスク装置128から、あるいはネットワーク100を介して認証付きの電子文書28が読み込まれる(V1)。次に、電子文書28から認証データである見出し付き暗号データ27が取出される(V2)。さらに見出し付き暗号データ27から暗号データ27Dが分離される(V3)。復号化手段30により、この分離された暗号データ27Dが外部認証機関の公開鍵29(#3)で復号化される(V4)。これによって、暗号データ31Dと第2の外部認証データ31Aの合成データが生成される。ここで認証データに改竄がなければ、暗号データ31Dは、暗号データ11D又は10Dと同じものであり、第2の外部認証データ31Aは、外部認証データ23Aと同じものである。

【0186】次に、暗号データ31Dと第2の外部認証データ31Aとが分離される(V5)。さらに、外部認証データ31Aから日付認証31A-Dが取出され、この2回目の外部認証機関99の認証が確認される(V6)。一方、暗号データ31Dは外部認証機関99の公開鍵13(#2)を使用して復号化手段14により復号され、暗号データ15Dと外部認証データ15Aの合成データが生成される(V7)。ここで認証データに改竄がなければ、暗号データ15Dは、暗号データ6D又は7Dと同じものであり、外部認証データ15Aは、1回目の外部認証データ7Aと同じものである。

【0187】次に、上記合成データが外部認証データ15Aと暗号データ15Dとに分離され(V8)、外部認証データ15Aからは日付認証データ15A-Dが取出される(V9)。これにより1回目の外部認証機関99による認証が確認される。

【0188】次に、暗号データ15Dが作成者の公開鍵16(#1)を使用して復号化手段17により復号化され、見出し付き特徴データ18が生成される(V10)。さらに、見出し18Hと特徴データ18Dとに分離される(V11)。

【0189】一方、認証付き電子文書28から、見出し付き暗号データ27が取り除かれ、この元の電子文書19から特徴抽出手段20により特徴データ21が抽出される(V12)。そして、ステップV11で分離された特徴データ18Dと、特徴データ21とが照合手段22により照合され、同一性判定データ22-Jが生成される(V13)。

【0190】照合結果である同一性判定データ22-Jにより、電子文書19と電子文書1とが同一かどうか判定され(V14)、不一致と判断された場合には表示装置111から不一致が表示される(V15)。一方、同一と判断された場合には、認証日付31A-D及び15A-Dとが表示され、さらに同一である旨の表示が行われる(V16)。こうして、改竄防止を強化した電子文書の同一性判定が終了する。

【0191】上述したように、本発明の実施の形態に係る電子文書の改竄防止システム及び方法は、外部認証機関99において期間をおいて2度に渡って認証され暗号化された認証付き電子文書28について、同一性を照合し外部認証を確認するようにしたので、改竄防止を強化した電子文書28の同一性の判定を容易に行う事ができる。また、暗号解読の恐れが有る年数を経過する前に更に新しい暗号による文書の改竄防止ができるので、長期間の電子文書保管を行っても、裁判の場で文書の正当性が証明できるようになる。

【0192】本実施形態では、電子文書28の如く1度の再認証(合計2回の外部認証)の電子文書28の同一性判定を行う実施例を説明したが、電子文書28を更に再認証した文書の同一性判定をしてもよい。認証の回数を重ねた場合は、復号の回数を重ねる事で電子文書の同一性判定が行える。

【0193】(第5の実施の形態)本実施形態では、第1又は第3の実施形態で説明した電子文書の改竄防止システムを利用した電子契約書作成システムについて説明する。

【0194】図13は本発明の第5の実施の形態の電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図であり、図4、図7、図9及び図11と同一部分には同一符号を付し、その説明を省略する。また、本実施形態のシステムには、図2及び図3に示す文書認証

システム101及び外部認証システム102が用いられており、本実施形態の独自の機能部分は、文書認証プログラム133あるいは外部認証プログラム134に修正が加えられたことによるものである。

【0195】この電子文書の改竄防止システムは、契約者の一方である甲が使用する文書認証システム101(以下、甲システム101aともいう)と、契約者の他方である乙が使用する文書認証システム101(以下、乙システム101bともいう)と、外部認証システム102とから構成されている。また、この電子文書の改竄防止システムは、甲乙間での契約を行うための電子契約書作成システムともなっている。なお、甲システム101aと、乙システム101bと、外部認証システム102とは図1に示すようにネットワークで接続されている。

【0196】甲システム101aは、秘密鍵4(#1)として甲の秘密鍵4(甲)を用い、また見出し付き暗号データ6を外部認証システム102に代えて乙システム101bに送信する。さらに、甲システム101aは、外部認証システム102から受け取る合成データ11として見出し付き暗号データ40を受け取り、電子文書1に付して電子契約書である認証付き電子文書41を作成する他、第1又は第3の実施形態の文書認証システム101と同様に構成されている。

【0197】一方、乙システム101bは、甲システム101aから受け取った見出し付き暗号データ6の中の暗号データ32Dに乙の認証データ32Aを付加した結合データを生成し、見出し付き認証データ32を作成する手段(図示せず)と、この結合データを乙の秘密鍵33(乙)で暗号化する暗号化手段34と、見出し付き認証データ32の見出し32H(35H)と暗号化手段34で暗号化された暗号データ35Dとを結合して電子署名35を作成する手段(図示せず)と、この電子署名35を外部認証システムにネットワークを介して送信する手段(図示せず)とを備える他、第1又は第3の実施形態の文書認証システム101と同様に構成されている。

【0198】なお、甲システム101aと乙システム101bは上記説明したそれぞれの各機能を組み合わせ、同一の処理が実行できるシステムとしてもよい。

【0199】また、外部認証システム102は、見出し付き認証データ7に代えて見出し付き認証データ36について図4と同様な処理を施すように構成され、さらに見出し付き暗号データを乙システム101bでなく甲システム101aに送信する他、第1又は第3の実施形態と同様に構成されている。すなわち、見出し付き認証データ36は図4の見出し付き認証データ7、暗号データ36Dは図4の暗号データ7D、外部認証データ36Aは図4の外部認証データ7A、見出し36Hは図4の見出し7Hに対応する。また、見出し付き暗号データ39は図4の合成データ10、見出し39Hは図4の見出し

10 H、暗号データ39 Dは図4の暗号データ10 Dに対応する。さらに、暗号化手段38は図4の暗号化手段9に対応し、秘密鍵37は図4の秘密鍵8に対応する。なお、暗号データ36 Dは、甲と乙のそれぞれにより暗号化された甲乙の認証データであり、暗号データ39はこの甲乙の認証データにさらに外部認証が与えられて暗号化されたものである。

【0200】次に、以上のように構成された本発明の実施の形態に係る電子文書の改竄防止システムの動作について図13及び図14を用いて説明する。

【0201】図14は本実施形態の電子文書の改竄防止システムの動作を示す流れ図である。

【0202】まず、甲システム101 aにおいて、外部記憶装置114、ハードディスク装置128から、あるいはネットワーク100を介して電子文書1が読み込まれる(W1)。次に電子文書1から見出し部分が取出され、金額情報と印紙税支払者名が記入され、その他必要事項を編集して見出し3 Hとする(W2)。

【0203】次に、電子文書1から特徴抽出手段2によって特徴データ3 Dが抽出される(W3)。さらに特徴データ3 Dが契約者甲の秘密鍵4 (甲)を用いて暗号化手段5によって暗号化され暗号データ6 Dが生成される(W4)。見出し3 H (6 H)と暗号データ6 Dとが結合され契約者甲の電子署名データである見出し付き暗号データ6が生成される(W5)。

【0204】この契約者甲の電子署名データは甲システム101 aから契約者乙の使用する乙システム101 bに電子文書1と共に送信される(W6)。なお、乙に電子文書1を送信するのは、乙が認証するに当たりその文書内容を確認できるようにするためである。

【0205】乙システム101 bにおいては、まず、契約者甲の電子署名(見出し付き暗号データ6)と電子文書1が受信される(W7)。この受け取った電子署名データが見出し32 Hと暗号データ32 Dとに分離される(W8)。

【0206】次に、暗号データ32 Dに乙の認証データ32 Aが結合されて結合データが生成される(W9)。この認証データ32 Aには乙の名前と日付が含まれる。次に暗号データ32 Dと認証データ32 Aが乙の秘密鍵33を用いて暗号化手段34によって暗号化され、暗号データ35 Dが生成される(W10)。

【0207】そして、見出し32 H (35 H)と暗号データ35 Dとが結合されることで甲と乙の電子署名35 (見出し付き暗号データ35)となる(W11)。この電子署名35は甲の秘密鍵4 (甲)で暗号化された部分と乙の秘密鍵33 (乙)で暗号化された部分が含まれ、更に見出し6 H及び認証データ32 Aに甲乙の名前が含まれるため、実質的に両者の電子署名となるものである。また、見出し35 Hあるいは暗号データ35 Dに甲乙の正規の電子署名を含ませるようにしてもよい。

【0208】こうして生成された甲と乙の電子署名35は外部認証機関99の外部認証システム102にネットワーク100を介して送信される(W12)。

【0209】外部認証システム102においては、甲と乙の電子署名35が受信される(W13)。次に、甲と乙の電子署名35が見出し36 Hと暗号データ36 Dとに分離される(W14)。さらに暗号データ36 Dに外部認証機関の外部認証データ36 Aが結合される(W15)。外部認証データ36 Aには外部認証機関99の名前と日付および印紙税支払い済の記事が含まれる。印紙税の支払については、予め甲が外部認証機関99との間で契約をしておく。

【0210】次に、暗号データ36 Dと認証データ36 Aとが外部認証機関99の秘密鍵37を用いた暗号化手段38によって暗号化され、暗号データ39 Dが生成される(W16)。さらに、見出し36 H (39 H)と暗号データ39 Dが結合され甲乙及び外部認証機関99の電子署名である見出し付き暗号データ39が完成する(W17)。この電子署名がネットワーク経由で甲システム101 aに送信される(W18)。

【0211】甲システム101 aにおいては、電子署名である見出し付き暗号データ39を見出し付き暗号データ40として受け取る(W19)。そして、この電子署名である見出し付き暗号データ40が電子文書1と合成されて電子契約書41 (認証付き電子文書41)が完成する。

【0212】上述したように、本発明の実施の形態に係る電子文書の改竄防止システム及び方法は、甲と乙と外部認証機関99とでそれぞれの秘密鍵で認証データを暗号化するようにしたので、作成された電子契約書に対する改竄を防止することができ、かつこれを証拠能力のある電子文書とすることができる。

【0213】つまり、電子契約書の改竄を行うとその電子文書1の有する特徴データが変化すること、最初に抽出された特徴データ3 Dが契約者の甲乙および外部認証機関の全員で暗号化されている事によって電子契約書の改竄を行うと必ず発見できることから、紙の代わりに電子文書での契約が可能になるものである。さらに、従来の紙の文書では改竄の有無を判定するには高度な技術が必要とされたが、本発明になる電文文書の改竄防止システムでは容易に改竄の有無を証明できる。また、電子化により保管場所が削減されると共に遠隔地への電送が瞬時に行えるようになり、コンピュータによる検索が行えるようになる。

【0214】加えて紙の契約書では字句の誤りを訂正する為に捨て印を押す悪習があったが、電子化により、契約者間で瞬時に文書のやり取りが可能になるので、捨て印を押さなくても直ちに訂正して再署名が可能と成り、契約者間のトラブルの発生を防止できる。電子署名35

に契約金額、印紙税支払者名が記載されているので、外部認証機関に電子文書そのものを送る必要が無く、秘密としたい事項が有る場合でも電子契約書を使用できる。

【0215】また、本実施形態では、電子文書1から特徴データを取り出して、これに甲乙、外部認証機関の認証を与えるようにしたが、本発明はこのような場合に限られるものでない。例えば元の電子文書1自体に文書作成者の関係者や上司が上司印等に相当するデータを付加し、当該上司印が付加された電子文書1から特徴データ3Dを取り出すようにすれば、実質的にその上司の認証をも付与された電子文書1を取り出すことが可能となる。元の電子文書を改竄すれば特徴データが変化するからである。

【0216】さらに、例えば本実施形態では、契約者が甲と乙の2人である場合を説明したが、本発明はこのような場合に限られるものではない。例えば契約者が甲、乙、丙の3者になる場合には、図13での乙のステップが丙に付いても繰り返し行われるようにすれば3人が契約者の認証が入った上記と同様な電子契約書を作成することができる。また、契約者に更に丁がいる場合には丁に付いてもこの乙のステップを繰り返し行えばよい。従って、契約者の人数には、かかわらず電子契約書を作成し使用できることとなる。

【0217】(第6の実施の形態)本実施形態では第5の実施形態で作成した電子契約書が真正なものであることを確認し、また契約者や外部認証機関の付した各認証日付等の認証情報を取り出すシステムについて説明する。

【0218】図15は本発明の第6の実施の形態の電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図であり、図4、図7、図9、図11及び図13と同一部分には同一符号を付し、その説明を省略する。また、本実施形態のシステムには、図6に示す認証文書認証システム103が用いられており、本実施形態の独自の機能部分は、認証文書確認プログラム135に修正が加えられたことによるものである。

【0219】この電子文書の改竄防止システムは、図1に示した認証文書確認システム103として構成されるものであり、電子契約書の照合システムでもある。

【0220】認証文書確認システム103は、電子契約書41(認証付き電子文書41)に付された見出し付き暗号データ40に対し、外部認証機関99の公開鍵42(認)、契約者乙の公開鍵45(乙)及び契約者甲の公開鍵48(甲)による復号を行い、外部認証機関の認証事実及び認証日付、乙の認証事実及び認証日付を取り出して認証確認を行うとともに、特徴データ50を取出し、一方、見出し付き暗号データ40を取り除いた電子文書1から特徴データ52を取出し、両特徴データ50、52を照合して同一性判定を行うようになっている。

【0221】このために電子文書の改竄防止システムには、電子契約書41から見出し付き暗号化データ40を取り出す手段(図示せず)と、これに含まれる暗号データ40Dを外部認証機関の公開鍵42(認)で復号する復号化手段43と、復号化手段43により復号化された外部認証データ44Aから外部認証機関の認証事実と認証日付を日付認証44A-Dとして取り出す手段(図示せず)と、復号化手段43により復号化された暗号データ44Dを乙の公開鍵45(乙)で復号化する復号化手段46とが設けられている。さらに、復号化手段46により復号化された乙の認証データ47Aから乙の認証事実と認証日付を日付認証47A-Dとして取り出す手段(図示せず)と、復号化手段46により復号化された暗号データ47Dを甲の公開鍵48(甲)で復号化する復号化手段49とが設けられている。一方、電子契約書41から見出し付き暗号化データ40が除かれた元の電子文書1から特徴抽出を行って特徴データ52を生成する特徴抽出手段51と、この特徴データ52と復号化手段49により復号化された特徴データ50Dとを照合して電子文書の同一性判定53-Jを行う照合手段53とが設けられている。

【0222】次に、以上のように構成された本発明の実施の形態に係る電子文書の改竄防止システムの動作について図15を用いて説明する。

【0223】まず、外部記憶装置114、ハードディスク装置128から、あるいはネットワーク100を介して電子契約書41が読み込まれ、認証データである見出し付き暗号データ40が取出される。この見出し付き暗号データ40から暗号データ40Dが取出され、外部認証機関の公開鍵42を用いて復号化手段43により復号化され暗号データ44Dと認証データ44Aが生成される。暗号データ44Dは図13の暗号データ36Dに対応するもので、外部認証データ44Aは図13の外部認証データ36Aに対応するものである。

【0224】外部認証データ44Aからは日付認証44A-Dが取出される。暗号データ44Dは契約者乙の公開鍵45を用いて復号化手段46によって復号化され、暗号データ47Dと認証データ47Aとが取出される。暗号データ47Dは図13の暗号データ32Dに対応し、認証データ47Aは図13の乙の認証データ32Aに対応する。

【0225】認証データ47Aからは乙の日付認証47A-Dが取出される。暗号データ47Dは契約者甲の公開鍵48を用いて復号化手段49によって復号化され特徴データ50Dが取出される。

【0226】一方電子文書41から認証データ40を取り除いたデータは電子文書1のデータに相当する。電子文書1に相当するデータから特徴抽出手段51によって特徴を抽出して特徴データ52が得られる。

【0227】照合手段53で特徴データ50Dと特徴データ52を照合して同一性判定を行うようになっている。

ータ52とが比較照合され、同一性判定53-Jが得られる。同一性判定53-Jが同一を示していれば電子文書の改竄は行われていないが、そうでない時には改竄が行われている。

【0228】また、甲作成の電子文書1に対する外部認証機関及び乙の認証事実と、認証日付が表示されることになり、契約書についての正当性が確認される。

【0229】上述したように、本発明の実施の形態に係る電子文書の改竄防止システム及び方法は、特徴データ50D、52による同一性判定及び甲作成の電子文書1に対する外部認証機関及び乙の認証事実並びに認証日付が確認されるので、電子契約書の同一性の判定を効果的に行う事ができ、裁判の場で文書の正当性が証明できるようになる。

【0230】なお、本実施形態では、契約者が甲と乙の2者の場合を説明したが、本発明はこの場合に限られるものではない。契約者が、甲、乙、丙の3者になる場合には図15での乙のステップが丙に付いても繰り返し行われるだけでよい。さらに契約者に更に丁がいる場合は丁に付いても乙のステップを繰り返し行えばよい。従って、契約者の人数にはかかわらない、複数人の間でかわされた電子契約書を確認することができる。

【0231】（第7の実施の形態）本実施形態は、上記各実施形態における例えば図4や図7の見出し11Hの編集手段の具体的な例を説明するとともに、認証付き電子文書12を表示あるいは印刷させるときの表示編集手段について説明する。

【0232】図16は本発明の第7の実施形態の電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図であり、図4、図7、図9、図11、図13及び図15と同一部分には同一符号を付し、その説明を省略する。本実施形態のシステムには、図2に示す文書認証システム101、あるいは図6に示す認証文書確認システム103が用いられている。本実施形態の独自の機能部分は、文書認証プログラム133あるいは認証文書確認プログラム135に修正が加えられたことによるものである。

【0233】この電子文書の改竄防止システムは、図1に示す文書認証システム101、あるいは認証文書確認システム103に以下に説明する手段が付加されてなる。なお、以下、文書認証システム101の場合を例にとって説明する。

【0234】本実施形態の文書認証システム101では、第1、第3、第5実施形態と同様な構成の他、表示印刷手段を備え、また、見出しの編集手段が具体的に示される。

【0235】見出しの編集手段には、見出し11Hを編集する際に、印鑑等が押された表示物をイメージ情報である印影54として取り込むスキャナ115（図2等）と、この印影54を電子印鑑60の一部に加える手段

（図示せず）と、印影54から特徴抽出して特徴データを生成する特徴抽出手段55と、特徴データ56を秘密鍵4で暗号化する暗号化手段58と、暗号化された暗号化印影59を電子印鑑60の一部に加える手段（図示せず）と、電子印鑑60に名前等を加える入力手段（入力装置112）と、完成した電子印鑑60を見出し11H（3H）として見出し付き特徴データ3（図16では合成データ11）に加える手段（図示せず）とが設けられている。なお、電子印鑑60は、印影54と暗号化印影59と所有者の名前を合成してなるものである。

【0236】一方、表示印刷手段には、合成データ11の見出し11Hから日付・署名・印影情報61を取り出す手段（図示せず）と、これらのデータを表示領域内に収まるように整形する手段62と、一方、認証付き電子文書12から電子文書1とを取り出す手段（図示せず）と、取り出された電子文書1の中に記載されるタグ及び表示領域情報1Tに整形された日付・署名・印影情報を重ね合わせる手段（図示せず）と、この重ね合わされた表示文書63を印刷あるいは表示する手段（表示装置111、印刷装置113）とが設けられている。

【0237】次に、以上のように構成された本発明の実施の形態に係る電子文書の改竄防止システムの動作について図16、図17、図18及び図19を用いて説明する。

【0238】まず電子印鑑60を生成する処理を図16および図17により説明する。

【0239】図17は本実施形態の電子文書の改竄防止システムの電子印鑑生成処理を示す流れ図である。

【0240】まず、電子印鑑の所有者名が入力装置112により入力される（X1）。次に印影データ54が読込まれる（X2）。印影データは紙に印鑑を押したものをスキャナ115で読み取り電子化したものが用いられる。

【0241】次に、印影データ54から特徴抽出手段55で特徴が抽出され特徴データ56が生成される（X3）。特徴データ56が所有者の秘密鍵4を使用した暗号化手段58により暗号化され暗号化印影59が生成される（X4）。印影データ54、暗号化印影59及びステップX1で入力した所有者名が一つのデータとして纏められ電子印鑑60が生成される（X5）。そして、電子印鑑60が第1の実施の形態の図1の見出しデータ3Hに入れられる。この結果図16の認証付き電子文書12の見出し11Hに電子印鑑60のデータが保存されることとなる（X6）。

【0242】次に改竄を防止した電子印鑑の照合処理を図18により説明する。

【0243】図18は本実施形態の電子文書の改竄防止システムの電子印鑑照合処理を示す流れ図である。

【0244】この照合処理は、電子文書1自体の同一性判定と別途に行われるものであり、見出し11Hに含ま

れる電子印鑑（電子署名）の正当性を評価するものである。なお、この処理の手段は特に図16では示していないが、その手段は文書認証プログラム133あるいは認証文書確認プログラム135とシステムのハードウェアで実現されるものであり、図18で示される処理を実現するものである。

【0245】まず、所有者名が入力される（Y1）。所有者名に従いその所有者の公開鍵が外部記憶装置114、ハードディスク装置128から、あるいはネットワーク100を介して読込まれる（Y2）。次に、電子印鑑60の中にある暗号化印影が公開鍵を用いて復号化される（Y3）。

【0246】一方、電子印鑑60の中にある印影データから特徴抽出が行われる（Y4）。次に、ステップY3で復号化した特徴データとステップY4で抽出した特徴データとの照合が行われる（Y5）。

【0247】この照合結果の判定が行われ（Y6）、印鑑が不一致であれば表示装置111にその旨表示される。一方、印鑑が一致していればその旨が表示される。

【0248】次に電子文書に電子印鑑や日付を重ね合わせて表示または印刷できるように、文書及び見出しを編集する処理を図16および図19により説明する。

【0249】図19は本実施形態の電子文書の改竄防止システムの文書見出し編集処理を示す流れ図である。

【0250】まず、電子文書1の編集が行われる（Z1）。この処理は電子文書1そのものの作成作業でありシステム使用者による作業である。さらに電子文書1にシステム使用者による作業で表示領域が設定される（Z2）。この段階で日付・署名・印影情報を表示する場所が決められる。

【0251】次に電子文書1の内部にステップZ2作成した表示領域にタグおよび表示領域情報1Tを埋め込む（Z3）。

【0252】ここから見出し編集に入り、日付・署名・印影情報61が編集される（Z4）。さらに見出しデータ11Hに埋め込むタイトル情報が入力されるか、もしくは電子文書内のタイトル部分が指定されその値が見出し11Hに取り込まれる（Z5）。そして見出し11Hが保存される（Z6）。

【0253】次に、電子文書1が保存される（Z7）。なお、電子文書1には見出し11H自体が埋め込まれる訳ではないので、ステップZ3の電子文書1へのタグおよび表示領域情報1T埋め込みの後に直ちにステップX7の文書保存を行ってもよい。

【0254】以上の処理により、電子文書1のどの場合に日付・署名・印影情報61を表示したらよいかが記録されるので、電子文書1を表示または印刷する時には、図16で示したように、電子文書上に日付・署名・印影を重ね合わせて表示文書63とすることができる。

【0255】これにより、改竄を防止した電子文書12

に改竄を防止した電子印鑑60が付けられ、さらにこれらを重ね合わせた表示文書63として、表示または印刷されることになる。

【0256】上述したように、本発明の実施の形態に係る電子文書の改竄防止システム及び方法は、特徴抽出を行って暗号化した電子印鑑60を見出し3Hに加えるようにしたので、電子印鑑60の印影改竄の有無が判定でき、電子文書に改竄を防止した印影を張り付けることができる。

【0257】また、このように改竄を防止した印影を、改竄を防止した改竄の有無判定ができる電子文書と合わせて、表示や印刷ができるようにしたので、この改竄防止が保障された表示や印刷によって、従来の紙の文書と同様な運用が可能となる。従来の紙の文書と同じ運用が可能でありながら、伝送で文書を瞬時に遠隔地に送る事ができる為その効果は非常に大である。なお、この場合、表示文書63に表示される電子文書は、同一性判定及び認証確認を行ったものを用いればより効果的である。

【0258】なお、本実施形態では、1つの電子印鑑60を見出し3Hに入れる場合で説明したが、本発明はこれに限られるものではない。見出しデータは編集する事が可能である為、図4や図7における使用の外に、図13や図15の使用においても運用する事ができ、電子文書の中に甲の日付・署名・印影と乙の日付・署名・印影を入れる事ができる。この場合にも電子文書1そのものは改竄される事が無い事は言うまでもない。

【0259】さらに、以上の説明では紙に印鑑を押したものをスキャナ115で読取り電子化した印影を用いるとしたが、紙に手書きのサインをしてスキャナ115で読取り電子化した電子サインを用いてもよい。

【0260】（第8の実施の形態）本実施形態は、上記第1～第7の実施形態で使用される特徴抽出手段の構成動作の例を説明する。

【0261】図20は本発明の第8の実施の形態の電子文書の改竄防止システムにおける特徴抽出方法を説明するための図である。

【0262】また、図21は本実施形態の電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図であり、図4、図7、図9、図11、図13、図15及び図16と同一部分には同一符号を付し、その説明を省略する。また、本実施形態のシステムには、図2に示す文書認証システム101、あるいは図6に示す認証文書認証システム103が用いられている。本実施形態の独自の機能部分は、文書認証プログラム133あるいは認証文書確認プログラム135に修正が加えられたことによるものである。

【0263】この電子文書の改竄防止システムは、図1に示す文書認証システム101、あるいは認証文書確認システム103における特徴抽出手段として以下に説明

する手段が設けられて構成される。なお、以下、文書認証システム101の場合を例にとって説明する。

【0264】図21に示すように、文書認証システム101又は認証文書確認システム103の特徴抽出手段2(20, 51, 55)は、電子文書1から特徴データ3Dを生成する。

【0265】この特徴抽出手段2には、データS__sumを格納する部分とデータIS__sumを格納する256個の配列と、図示しない処理手段とが設けられている。この処理手段は以下に説明する処理を実現する機能実現手段である。

【0266】まず、図20は特徴抽出手段のデータの流れを示している。

【0267】同図において、電子文書やファイル等のデータそのもの、すなわちStreamは、電子文書データ並びSをなしている。この電子文書データ並びSは、256バイトずつに区切られた電子文書データ並び部分S1、S2、S3、...、Snにより構成される。

【0268】このStreamから生成されるS__sum__streamは、合計データ並びS__s__streamをなしている。この合計データ並びS__s__streamは、合計データ並び部分SS1、SS2、SS3、...から構成される。SS1は、S1、S2、S3、...、S256それぞれの合計値を256個のデータの並びとしたものである。同様に、SS2は、S257~S512それぞれの合計値をデータの並びとしている。

【0269】一方、StreamからはIntervalled Stringとして間隔を置いたデータ並びISが生成される。この間隔を置いたデータ並びISは間隔を置いたデータ並び部分IS1、IS2、IS3、...、ISnから構成される。ここで、IS1は、S1、S2、S3、...、S256の各先頭データを順次256個並べたものであり、IS2は、S1、S2、S3、...、S256の各2番目のデータを順次256個並べたものである。以下同様に、IS3~IS256が構成される。IS257は、S257~S512の各先頭データを順次256個並べたものである。以下同様である。

【0270】このIntervalled Stringから生成されるIS__sum__streamは、間隔を置いた合計データ並びIS__s__streamをなしている。この間隔を置いた合計データ並びIS__s__streamは、間隔を置いた合計データ並び部分ISS1、ISS2、ISS3、...から構成される。この間隔を置いた合計データ並び部分ISS1、ISS2、ISS3、...は、間隔を置いたデータ並び部分IS1~ISnから生成され、その生成方法は、S1~SnからSS1、SS2、SS3、...を生成する方法と同じである。

【0271】なお、最終的には、合計データ並びS__s__streamと間隔を置いた合計データ並びIS__s__streamとが特徴データ3Dとなる。

【0272】ここで、図20と図21との関係を説明すると以下の通りである。

【0273】S1は256バイトのデータの並びで、このS1のデータの合計値が図21のS__sumに格納され、S__sumの値がS__s__streamに出力される。S__s__streamはワード(16ビット)のデータの並びで256バイトの合計値を取っても桁落ちは発生しない。同様にS1に続くデータの並びS2に対しても合計値がS__s__streamに出力される。以下、S3からSnに至るまで同様に行われる。

【0274】IS1は256バイトのデータの並びでS1の先頭1バイト、S2の先頭1バイトS3の先頭1バイトと続き、S256の先頭1バイトまでが格納される。IS2は同様に256バイトのデータの並びでS1の2バイト目、S2の2バイト目、S3の2バイト目と続き、S256の2バイト目までが格納される。同様にIS3は同様に256バイトのデータの並びでS1の3バイト目、S2の3バイト目、S3の3バイト目と続き、S256の3バイト目までが格納される。IS256はS1の256バイト目、S2の256バイト目、S3の256バイト目と続き、S256の256バイト目までが格納される。IS1からIS256までのデータはそれぞれ合計が取られて、図21のIS__sum

[0]からIS__sum[255]に格納され、IS__sumの並びがIS__s__streamに出力される。IS__s__streamはワードのデータの並びで256バイトの合計値を取っても桁落ちは発生しない。

【0275】こうしてS__s__streamとIS__s__streamからなる特徴データが得られるが、次にこの処理のフローを図22で説明する。

【0276】図22は本実施形態の電子文書の改竄防止システムの特徴データ抽出の処理の一例を示す流れ図である。

【0277】まず、全てのデータが初期化される(A1)。次に電子文書データ並びSのデータが有るかどうか調べられる(A2)。

【0278】データが有る場合にはステップA3に移り、Sから1バイトが読込まれる。一方、データが無い場合にはステップA4に移り終了処理が行われる。

【0279】ステップA3でSから1バイトを読んだ後は、読んだ値がS__sumとIS__sum[i]に加算される(A5)。

【0280】次に、iが255かどうか調べられる(A6)。iが255でない場合にはiを1増加させ(A7)、ステップA2に戻る。一方、iが255の場合には(A6)、S__sumの値がS__s__streamに出力されiがゼロに戻される(A8)。

【0281】次に、jが255かどうか調べられる(A9)。jが255でない場合にはjを1増加させ(A10)、ステップA2に戻る。一方、jが255の場合には(A9)、IS_sum[1]からIS_sum[255]までの値をIS_streamに出力してjをゼロに戻し(A11)、ステップ2に戻る。

【0282】このような処理により、電子文書のデータが1バイトずつ順次読込まれ、全データが処理されるまで図20のデータ(S_stream, IS_stream)が生成されつづけ、特徴データ3Dとして出力される。

【0283】このS_stream及びIS_streamを特徴データとした場合、電子文書データ並びS(電子文書1や印影54等)のどの1バイトの値が変化してもS_streamの何処かの1ワードが変化する。また、電子文書データ並びSのどの2バイトを入れ替えてもIS_streamの何処かの1ワードが変化する。

【0284】例えば、S1のデータ部分内部でデータの入れ替えを行うと、S1の合計値は変化しないがIS_sum[0]からIS_sum[255]の何処かの値は必ず変化する。これによって電子文書1のどのデータが改竄しても改竄の事実が発見される。また、S1の256バイトのデータが1ワードに圧縮され、IS1の256バイトのデータが1ワードに圧縮されることから、元のデータの1/64のサイズにデータが圧縮される。また、このように生成される特徴データは、データの圧縮が一方方向性であり、特徴データから元のデータを再現する事はできない。

【0285】上述したように、本発明の実施の形態に係る電子文書の改竄防止システム及び方法は、特徴抽出手段により、図20に示すようなS_stream及びIS_streamを特徴データとして生成するようにしたので、元のデータのどの部分がどの様に変化してもその変化を発見することができる。また、特徴データは元のデータに比較してデータサイズが大幅に小さくなり取り扱いが容易である。また、特徴データの取出し方がシンプルで演算を高速にすることができる。

【0286】さらに、特徴データから元のデータを再現できないことから、外部認証機関99に電子文書1を開示したくない場合には、認証対象を不開示のまま電子文書の認証を行うことができる。特徴データを用いる方法では電子文書の認証にその文書自体の引き渡しが必要ないからである。

【0287】(第9の実施の形態)本実施形態は、上記第1～第7の実施形態で使用される特徴抽出手段の構成動作の他の例を説明する。

【0288】図23は本発明の第9の実施の形態の電子文書の改竄防止システムにおける特徴抽出方法を説明するための図であり、図20と同一部分には同一符号を付

してその説明を省略する。

【0289】また、本実施形態の電子文書の改竄防止システムには、図2に示す文書認証システム101、あるいは図6に示す認証文書認証システム103が用いられ、特徴抽出手段として以下に説明する手段が設けられている。なお、本実施形態の独自の機能部分は、文書認証プログラム133あるいは認証文書確認プログラム135に修正が加えられたことによるものである。

【0290】本実施形態における特徴抽出は、S_stream及びIS_streamが抽出されるまでは第8の実施形態と同様に行われる。また、S_streamからS_stream'、IS_streamからIS_stream'が生成され、これらのS_stream'及びIS_stream'が最終的な特徴データ3Dとして使用される。なお、S_stream'及びIS_stream'はロングワード(32ビット)で構成される。

【0291】具体的な処理としては以下ようになる。

【0292】まず、SS1等とISS1等を生成する手前までは第8の実施形態と同様である。第8の実施の形態では実際の処理においてはSS1等とISS1等を256ワード単位で区切らずにS_stream及びIS_streamとしてそのまま出力していた。これに対して図23においてはS1、S2、S3、...、Snを256バイトずつ合計して成る値の列を256ワードずつSS1、SS2...SS256の合計値のロングワードの列にしてS_stream'に出力する。また、IS1、IS2、IS3、...、IS256の合計値のロングワードの列をIS_stream'に出力する。

【0293】いいかえると、S_stream'には、SS1、SS2、...それぞれの合計値が順次データ並びとして出力され、同様に、IS_stream'には、ISS1、ISS2、...それぞれの合計値が順次データ並びとして出力される。

【0294】これによって、図20ではS_streamはワードのストリームであったが、図23ではS_stream'はロングワードのストリームとなる。同様に、図20ではIS_streamはワードのストリームであったが、図23ではIS_streamはロングワードのストリームとなる。これによりデータ量は更に1/128に圧縮され、最初の1/8192の大きさになる。

【0295】上述したように、本発明の実施の形態に係る電子文書の改竄防止システム及び方法は、特徴抽出手段により、図23に示すようなS_stream'及びIS_stream'を特徴データとして生成するようにしたので、第8の実施形態と同様な効果が得られる他、第8の実施形態の場合よりも更に特徴データ

をコンパクトなものとするができる。

【0296】なお、第9の実施形態では第8の実施形態に対してデータの256個毎の合計を1回余分に行っているが、1回だけでは無く更に繰り返してデータを圧縮してもよい。このようにすればより一層特徴データをコンパクトなものとするができる。

【0297】(第10の実施の形態)本実施形態は、上記第1～第7の実施形態で使用される特徴抽出手段の構成動作のさらに他の例を説明する。

【0298】図24は本発明の第10の実施の形態の電子文書の改竄防止システムにおける特徴抽出方法を説明するための図である。

【0299】また、図25は本実施形態の電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図であり、図4、図7、図9、図11、図13、図15及び図16と同一部分には同一符号を付し、その説明を省略する。また、本実施形態のシステムには、図2に示す文書認証システム101、あるいは図6に示す認証文書認証システム103が用いられている。本実施形態の独自の機能部分は、文書認証プログラム133あるいは認証文書確認プログラム135に修正が加えられたことによるものである。

【0300】この電子文書の改竄防止システムは、図1に示す文書認証システム101、あるいは認証文書確認システム103における特徴抽出手段として以下に説明する手段が設けられて構成される。なお、以下、文書認証システム101の場合を例にとって説明する。

【0301】図25に示すように、文書認証システム101又は認証文書確認システム103の特徴抽出手段2(20, 51, 55)は、電子文書1から特徴データ3Dを生成する。

【0302】特徴抽出手段2には、セバレータテーブル2T及び単語配列2Wが設けられている。

【0303】一方、図24において、電子文書1は単語とセバレータの並びで構成される。セバレータというのは、文書中において空白や句読点等の単語を分離するものである。単語配列2Wは単語のデータの並びとその順番で構成される。一方、特徴データ3Dは単語配列2Wのデータ並びの順番データの並びで構成される。

【0304】また、セバレータテーブル2Tは、予めセバレータとして使用するものを登録したものである。一方、単語配列2Wは、単語を格納する領域と配列の順番からなっている。

【0305】次に、以上のように構成された本発明の実施の形態に係る電子文書の改竄防止システムにおける特徴抽出処理について説明する。

【0306】まず、図24で示すように、単語とセバレータから構成された電子文書1の先頭から順次データが読み込まれ、セバレータとセバレータで区切られたデータが単語とみなされる。見つけた単語のうち新しいも

のが単語配列2Wに登録され、その単語の配列番号が特徴データ3Dに書き出される。すなわちこの配列番号の並びそのものが特徴データとなる。

【0307】つまり、特徴抽出手段2により読み込まれた1文字がセバレータテーブル2Tのデータと比較され、セバレータでなければ次の1文字が読み込まれる。順次読み込みが行われ、読み込みを続けて得られた文字列が単語として検出される。この場合に、当該文字列が新しい単語であるか否かが判定される。そして新しい単語の場合には文字配列2Wに登録し登録番号を特徴データ3Dとして書き出す。既に出てきた単語の場合にはその登録番号を特徴データ3Dに書き出す。

【0308】この処理を図26を用いてより具体的に説明する。

【0309】図26は本実施形態の電子文書の改竄防止システムの特徴データ抽出の処理の一例を示す流れ図である。

【0310】まず、全てのデータが初期化される(B1)。次に、電子文書1のデータがあるかどうか調べられ(B2)、データがある場合には1文字分が読み込まれる(B3)。データが無い場合には(B2)終了処理が行われる(B4)。

【0311】次に、読み込んだ1文字がセバレータかどうかセバレータテーブル2Tのデータとの比較により行われる(B5)。読み込んだ1文字がセバレータの場合には(B5)、セバレータテーブル2Tとセバレータの比較が行われる(B6)。一方、読み込んだ1文字がセバレータでない場合には(B5)、その文字をバッファに入れてステップB2に戻る(B7)。

【0312】ステップB6の後、配列2Wのテーブルデータ(ハッシュテーブル)とバッファデータの比較が行われる(B8)。なお、ステップB6はセバレータ自体の種類を決定するものであり、ステップB8はバッファの中に構成された単語の種類を決定するものである。

【0313】次に、ステップB6の結果よりテーブルデータ(配列2W)とセバレータが同じでない場合には(B9)、データがテーブル2Wに登録され(B10)ステップB11に移る。一方、同じ場合には(B9)、ステップB10を行わずにステップB11に移る。

【0314】ステップB11では、テーブルデータ(配列2W)とバッファデータが同じでない場合には、バッファデータがハッシュテーブル2Wに登録され(B12)、ステップB13に移動する。一方、同じ場合には(B11)ステップB12を行わずにステップB13に移動する。

【0315】そして、ステップB13では、特徴データ3DにステップB9～B12で決定されたセバレータと単語それぞれのテーブル番号が出力される。その後ステップB2に戻る。

【0316】以上により電子文書1の特徴がハッシュテ

ーブルのテーブル番号並びとして抽出され特徴データ3 Dとして得られる。

【0317】上述したように、本発明の実施の形態に係る電子文書の改竄防止システム及び方法は、特徴抽出手段により単語とセパレータのテーブル番号の並びを特徴データとして抽出するようにしたので、元のデータのどの部分がどの様に変化してもその変化を発見することができる。また、元のデータに比較してデータのサイズが大幅に小さくなり取り扱いが容易である。さらに特徴データから元のデータを再現できないことから、外部認証機

関に電子文書を開示したくない場合であっても電子文書の認証を行うことができる。

【0318】(第11の実施の形態)本実施形態は、第1～第7の実施形態で説明した電子文書の改竄防止システムにおける各文書認証システム101、外部認証システム102及び認証文書確認システム103を使用するにあたり、そのシステム使用者を確認するための情報を生成し、また、各システムで用いられる暗号鍵(秘密鍵、公開鍵等)を生成する手段について説明する。

【0319】図27は本発明の第11の実施の形態の電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図であり、図4、図7、図9、図11、図13、図15及び図16と同一部分には同一符号を付し、その説明を省略する。また、本実施形態のシステムには、図2に示す文書認証システム101、図3に示す外部認証システム102あるいは図6に示す認証文書確認システム103が用いられている。本実施形態の独自の機能部分は、文書認証プログラム133、外部認証プログラム134あるいは認証文書確認プログラム135に修正が加えられたことによるものである。

【0320】この電子文書の改竄防止システムは、図1に示す文書認証システム101、外部認証システム102あるいは認証文書確認システム103と同様な構成に、以下に各手段が付加されて構成される。なお、以下、文書認証システム101の場合を例にとって説明する。

【0321】図27に示す文書認証システム101は、システム使用者の指紋を読み取って特徴抽出を行い、この特徴データ67、別途入力されたパスワード68及び乱数を用いて暗号鍵71、74、75、77S、77Kを生成するとともに、さらに使用者氏名、ID(識別情報)、パスワード、指紋及び生成した暗号鍵等から本人認証データ78を生成するものである。この本人認証データ78は、後述する第12の実施形態においてシステム使用者を確認するのに用いられる。

【0322】この本人認証データ78を生成するために文書認証システム101には、指紋読取り機64と、イメージデータとして読み取られた指紋65から特徴データ67を抽出する特徴抽出手段66と、入力装置112から入力されたパスワード68及び氏名・ID69のう

ちパスワード68と特徴データ67から暗号鍵71を生成する暗号鍵生成手段70と、乱数発生器72と、乱数発生器72から発生した乱数、パスワード68及び特徴データ67から秘密鍵74及び公開鍵を生成する秘密鍵公開鍵生成手段73と、暗号鍵71及び秘密鍵74から暗号化秘密鍵77S及び暗号化暗号鍵77Kを生成する暗号化手段とが設けられている。さらに、文書認証システム101には、指紋65、暗号化秘密鍵77S、暗号化暗号鍵77K、パスワード68及び氏名・ID69を取り込み、指紋78F、暗号化秘密鍵78S、暗号化暗号鍵78K、パスワード78P及び氏名・ID78Nからなる本人認証データ78を作成する手段(図示せず)とが設けられている。

【0323】次に、以上のように構成された本発明の実施の形態に係る電子文書の改竄防止システムの動作について図27及び図28を用いて説明する。

【0324】図28は本実施形態の電子文書の改竄防止システムの動作を示す流れ図である。

【0325】本動作は文書認証システム101のシステム起動時等における本人認証用データを作成する手続きである。

【0326】このためにまず、入力装置112により、最初に氏名・IDデータ69とパスワード68が入力されてシステムが起動される(C1)。次に、指紋読取り機64が起動され指紋が読取られる(C2)。これにより、指紋データ65が得られる。

【0327】次に、指紋データ65から特徴抽出手段66によって特徴データ67が抽出される(C3)。さらにパスワード68と特徴データ67とが使用され暗号鍵生成手段70により暗号鍵71が生成される(C4)。

【0328】次に、パスワード68、乱数発生器72および特徴データ67が使用され秘密鍵公開鍵生成手段73により秘密鍵74と公開鍵75が生成される(C4)。本実施形態では秘密鍵公開鍵生成手段73としてRSA方式に対応したものをを用いている。なお、DES等を用いてもよい。

【0329】次に、暗号鍵71と秘密鍵74とが暗号化手段76により暗号化され暗号化秘密鍵77Sと暗号化暗号鍵77Kが生成される(C6)。なお、本実施形態では、暗号化手段76は共通鍵暗号方式の一つであるDES方式を用いており、暗号鍵71をその暗号鍵としている。暗号鍵71については自分で自分を暗号化する事(暗号化暗号鍵77Kの生成)になる。

【0330】そして、指紋データ65、暗号化秘密鍵77S、暗号化暗号鍵77K、パスワード68及び氏名・ID69が本人認証データ78として一つにまとめられる(C7)、ハードディスク装置128等に格納される(C8)。また、この情報のうち、公開鍵75は所定の場所に登録されることになる(C9)。

【0331】上述したように、本発明の実施の形態に係

る電子文書の改竄防止システム及び方法は、指紋データを元にして暗号鍵を生成するようにしたので、本人認証を確実なものとして行うことができるとともに、本人が暗号鍵のデータ自体を知る必要がなく、システムの利用を簡便なものとして行うことができる。また、暗号鍵そのものが暗号化されていること、秘密鍵が暗号化されている事からたとえ本人認証データ78を盗まれる事が有っても暗号鍵と秘密鍵の内容を知る事はできず、極めて安全な情報管理を行うことができる。

【0332】なお、本実施形態では暗号鍵生成手段70にパスワードを必要としたが、本発明はこのような場合に限られるものではない。例えば特徴データ67のみから暗号鍵を生成しても同様の効果が得ることができる。また例えば秘密鍵公開鍵生成手段73にパスワード68と乱数発生器72を必要としていたが、何れか一方が無くても、また両方が無くても同様の効果が得ることが可能である。

【0333】さらに、本実施形態では、暗号鍵等の生成に指紋を用いることとしたが、本発明は指紋に限られるものでなく、声紋や虹彩等、本人を特定できるものであれば、種々の生体データを利用することができる。

【0334】(第12の実施の形態) 本実施形態は、第11の実施形態のシステムで登録したシステム使用者に当該システムが使用できるようにする。すなわち、第1～第7の実施形態で説明した電子文書の改竄防止システムにおける各文書認証システム101、外部認証システム102及び認証文書確認システム103を使用するにあたり、そのシステム使用者を確認し、また、各システムで用いられる暗号鍵(秘密鍵、公開鍵等)を使用可能とする手段について説明する。

【0335】図29は本発明の第12の実施の形態の電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図であり、図4、図7、図9、図11、図13、図15、図16及び図27と同一部分には同一符号を付し、その説明を省略する。また、本実施形態のシステムには、図2に示す文書認証システム101、図3に示す外部認証システム102あるいは図6に示す認証文書確認システム103が用いられている。本実施形態の独自の機能部分は、文書認証プログラム133、外部認証プログラム134あるいは認証文書確認プログラム135に修正が加えられたことによるものである。

【0336】この電子文書の改竄防止システムは、図1に示す文書認証システム101、外部認証システム102あるいは認証文書確認システム103と同様な構成に、以下に各手段が付加されて構成される。なお、以下、文書認証システム101の場合を例にとって説明する。

【0337】図29に示す文書認証システム101は、正当な使用権限を有する者が電子文書の改竄防止システムを使用したい場合に、パスワード68及び指紋65を

入力させ、これと第11の実施形態で生成された本人認証データ78に予め格納された指紋78F、パスワード78Pとにより本人確認を行った後、指紋78F、パスワード78P及び暗号化暗号鍵78Kから暗号鍵を取出し、さらにこの暗号鍵により暗号化秘密鍵78Sを復号して秘密鍵4を取出して、第1～第7の実施形態の電子文書の改竄防止システムを使用可能な状態にする。

【0338】このために文書認証システム101には、指紋読取り機64と、読み取られた指紋65と本人認証データ78内の指紋78Fとを照合する照合手段81と、入力装置112から入力されたパスワード68と、本人認証データ78内のパスワード78Pとを照合する照合手段80と、照合手段80及び81の結果から本人認証の判定を行う判定ロジック手段82とが設けられている。さらに、文書認証システム101には、判定ロジック手段82から本人が認証された旨を受けると指紋78Fから特徴データ67を抽出する特徴抽出手段66と、特徴データ67及びパスワード78Pから暗号鍵71を生成する暗号鍵生成手段70と、暗号化暗号鍵78Kを暗号鍵71で復号して暗号鍵84を取り出す復号手段83と、暗号鍵71と暗号鍵84とを照合して正しく暗号鍵71が取り出されたことを確認する照合手段85と、取り出された暗号鍵71を用い暗号化秘密鍵78から電子文書の改竄防止システム(図4等)で使用する秘密鍵4を取り出す復号手段86と、氏名・ID78N等を表示する表示手段79とが設けられている。

【0339】次に、以上のように構成された本発明の実施の形態に係る電子文書の改竄防止システムの動作について図29及び図30を用いて説明する。

【0340】図30は本実施形態の電子文書の改竄防止システムの動作を示す流れ図である。

【0341】本動作は生体データ等の入力により本人認証用データに基づいて文書認証システム101のシステム起動時等における本人確認及び秘密鍵生成を行う手続きである。

【0342】まず、入力装置112から本人認証を行う為に名前が入力されると、ハードディスク装置128から本人認証データ78が読み込まれ、表示手段111により氏名・IDが表示される。システム使用者は、氏名・IDを確認してパスワード68を入力する(D1)。

【0343】次に、本人認証データ78中のパスワード78Pと今入力したパスワード68とが照合される(D2)。この照合が一致すれば指紋読取り機64で指紋が読取られ、イメージデータである指紋65が生成される(D3)。

【0344】次に指紋照合手段81により指紋78Fと読み取った指紋65とが照合される(D4)。照合が一致すれば(D4)、本人認証データ78から指紋78Fが取り出され特徴抽出手段66により特徴抽出されて特徴データ67が生成される(D5)。ここで読み取った

指紋65を用いず本人認証データ78内の指紋78Fを用いるのは、読み取った指紋65は1ビットも違わずに指紋78Fと一致することは有り得ず、より取るたびに若干の違いを生じるためである。一方、特徴抽出では第8～第10の実施形態で説明したようにわずかな違いがあっても異なる特徴データとして抽出されるので、第11の実施形態で取り出した指紋そのものを使用して暗号鍵71を取り出そうとするものである。

【0345】つまり、この特徴データ67とパスワード78Pが使用され暗号鍵生成手段70により暗号鍵71が生成される(D6)。次に本人認証データ78から暗号化暗号鍵78Kが取り出されステップD6で生成した暗号鍵71によって復号される(D7)。

【0346】さらにステップST7で復号した暗号鍵84とステップST6で生成した暗号鍵71が照合手段85で照合される(D8)。照合が一致すれば最終的に本人の認証ができたことみなされる。そして、本人認証データ78から暗号化秘密鍵78Sが取り出され暗号鍵71を用いた復号手段86により復号されて秘密鍵4が生成される(D9)。

【0347】こうして電子文書の改竄防止システムが使用可能になり、文書読取り(D10)、特徴抽出(D11)、秘密鍵4による特徴データの暗号化(D12)等といった各実施形態で説明した処理が行われることとなる。

【0348】上述したように、本発明の実施の形態に係る電子文書の改竄防止システム及び方法は、システム使用者の指紋65を読み取り、これと本人認証データ78とを照合するようにしたので、本人認証データ78から秘密鍵4を取り出す事ができる。ここで、本人認証データ78内において秘密鍵と暗号鍵は暗号化されて保存されているので、仮に本人認証データを盗まれても秘密鍵と暗号鍵が知られる事はできず非常に安全である。また、暗号鍵は本人認証データの中に保存された指紋78Fから生成されるので確実に同じ暗号データを再現できると共に、暗号データそのものを誰にも知らせる必要が無く極めて安全である。

【0349】なお、本実施形態では暗号鍵生成手段70にパスワードも使用していたが、第11の実施形態における変形例に対応させて、特徴データ67だけで暗号鍵を生成するようにしてもよい。本実施形態では指紋を用いて暗号化された鍵について取り扱ったが、本発明は指紋に限られるものでなく、声紋や虹彩等、本人を特定できるものであれば、種々の生体データを利用して本人認証を行うようにしてもよい。

【0350】(第13の実施の形態) 本実施形態は、第11及び第12の実施形態のシステムにおける指紋読取り機64で読み取った情報から指紋65を生成する手段と、指紋65から特徴抽出を行う特徴抽出手段66とについて説明する。

【0351】図31は本発明の第13の実施の形態の電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図であり、図4、図7、図9、図11、図13、図15、図16、図27及び図29と同一部分には同一符号を付し、その説明を省略する。また、本実施形態のシステムには、図2に示す文書認証システム101、図3に示す外部認証システム102あるいは図6に示す認証文書認証システム103が用いられている。本実施形態の独自の機能部分は、文書認証プログラム133、外部認証プログラム134あるいは認証文書確認プログラム135に修正が加えられたことによるものである。

【0352】この電子文書の改竄防止システムは、図1に示す文書認証システム101、外部認証システム102あるいは認証文書確認システム103と同様な構成に、以下に各手段が付加されて構成される。なお、以下、文書認証システム101の場合を例にとって説明する。

【0353】図31に示す文書認証システム101は、指紋読取り機64からの指紋原データ87Fから指紋65を生成する指紋データ抽出手段87と、指紋65から特徴データ67を抽出する特徴抽出手段66とによって構成されている。

【0354】指紋データ抽出手段87には、境界抽出手段87Aと、エンボス手段87Eと、輪郭抽出手段87Lと、2値化手段87Bとが設けられている。

【0355】一方、特徴抽出手段66には、指紋65からデータ66SDを切り出す領域切り出し手段66Sと、切り出されたデータ66SDと予め用意されたパターン66Pとをマッチングさせるマッチング手段66Mと、マッチング手段66Mにより生成された一桁分データ66Dから特徴データ67を生成する手段(図示せず)とが設けられている。

【0356】次に、以上のように構成された本発明の実施の形態に係る電子文書の改竄防止システムの動作について図31、図32、図33、図34及び図35を用いて説明する。

【0357】図32は指紋データ65の一例を示す図である。

【0358】図33は指紋データ65から矩形領域に切り出したデータ66SDの一例を示す図である。

【0359】図34はマッチングさせるパターンの例の一部分を示した図である。

【0360】図35は本実施形態の電子文書の改竄防止システムの動作を示す流れ図である。

【0361】図35において、まず、指紋読取り機64により指紋についてのデータが読取られ、指紋原データ87Fが得られる(E1)。

【0362】次に境界抽出手段87Aにより指紋データの境界が明確にされ(E2)、さらにエンボス手段87

Eにより境界を明確にしたデータのエンボスが取られる(E3)。次にデータの輪郭抽出が行われ(E4)、さらに抽出データが2値化されて指紋データ65を得る(E5)。図32にこの様にして得た指紋データ65のサンプルが示される。

【0363】次に、領域切り出し手段66Sによって領域が指定されつつデータ66SDの切り出しが行われる(E6)。この様にして切り出したデータのサンプルが図33に示される。

【0364】次にマッチング手段66Mによりデータ66SDとパターンデータ66Pとのパターンマッチングが行われる(図35E7)。図34にマッチングを行うパターンの一例が示される。パターンマッチングが成立すると、マッチング手段66Mからマッチングデータを取り出してこれを1桁データ66Dとする(E8)。

【0365】次に、特徴データを生成するのに必要な桁数が指紋65から読み出されたかが調べられ、まだデータが有る場合にはステップE6～E8が繰り返される(E9)。必要な桁数を読み終わると(E9)、1桁データ66Dから生成される特徴データ67が出力される。

【0366】以上により指紋データ65から暗号鍵を生成する為の特徴データ67の生成が行われる。

【0367】上述したように、本発明の実施の形態に係る電子文書の改竄防止システム及び方法は、指紋データ65から暗号鍵を生成する為の特徴データ67を生成することができるので、これを第11及び第12の実施形態における本人認証及び秘密鍵復号システムに利用でき、その効果は非常に大きい。

【0368】[第14～第17の実施形態についての説明]上記第1～第13の実施形態に説明した発明によれば、文書作成した本人以外に外部認証機関の認証を追加することで、作成した本人による文書改竄をも防止することができ、重要書類を電子化することが可能となる。

【0369】しかし、作成した文書に別の作者が一部変更を加えて、新しい文書にする時には、元の作者と新しい作者及び外部認証機関が再び認証を行なう必要がある。

【0370】そこで、以下の第14～17の実施形態においては、改竄防止の為に認証を行なった電子文書及びデータの変更に、オリジナルの作者以外の変更に、当該オリジナル作者の認証を維持しつつ変更電子文書の再認証を可能とする方法及びシステムについて説明する。すなわち以下の実施形態では、複数の作者が複数の時期に渡って作成した電子文書の変更履歴を明らかにしつつ信用性を付与すると共に取り扱い性を高め、従来紙でしかできなかった履歴文書等の変更文書の電子化を実現する。

【0371】図36は本発明の第14～第17の実施形態における文書変更を含んだ電子文書の改竄防止シス

ム及び方法の全体的な構成を示す図である。

【0372】同図に示すように、公衆回線や専用回線を用いたネットワーク1100が構成され、当該ネットワークに文書認証システム1101や外部認証機関1099の外部認証システム1102、文書変更認証システム1103、認証文書確認システム1104が接続されている。

【0373】文書認証システム1101は、第1～第13の実施形態で説明した文書認証システム1101と同様に構成されたシステムである。外部認証システム1102は文書認証システム1101から認証すべき情報を受信して、認証した結果を返信する。また、外部認証システム1102はネットワーク1100を介して、文書変更認証システム1103から認証すべき情報を受信して、認証した結果を返信する。

【0374】文書認証システム1101、文書変更認証システム1103、認証文書確認システム1104は複数存在してよく、異なった使用者によって使用される。

【0375】また、文書認証システム1101、外部認証システム1102、文書変更認証システム1103、及び認証文書確認システム1104は、ワークステーションやパーソナルコンピュータなどの計算機に表示装置、入力装置、あるいは例えば指紋読取装置、スキャナ装置などを付加したものであり、基本的には動作プログラムが異なる事で異なる各機能を実現する。従って、文書認証システム1101、文書変更認証システム1103、認証文書確認システム1104は一つの計算機上に構成される場合も有る。

【0376】さらに、文書変更認証システム1103及び外部認証システム1102とを同一計算機、あるいはLAN等で接続される計算機上に構成させ、外部認証機関において、認証作業の全てを行うようにする事も可能である。

【0377】本発明に関わる電子文書の変更認証システム及び方法は、これらの文書認証システム1101、外部認証システム1102、文書変更認証システム1103及び認証文書確認システム1104を適宜組み合わせ、あるいはその一部機能を適宜組み合わせるものである。さらに本明細書では、便宜上、第1～第13の実施形態と第14～第17の実施形態とにわけて説明しているが、両実施形態グループに属する各システムを適宜組み合わせ、あるいはその一部機能を適宜組み合わせ又組み込むことも可能である。

【0378】また、上記場合はネットワークを介した情報の瞬時転送を前提とした場合を説明しているが、図36に示す様にフロッピーディスク等の記録媒体97、98を介して文書変更認証システム1101～外部認証システム1102間、あるいは文書認証システム1101～文書変更認証システム1103間、文書変更認証システム1103～認証文書確認システム1104間で必要

情報の交換を行う事も可能である。

【0379】全体的には以上のシステム構成を有する文書変更を含んだ電子文書の改竄防止システム及び方法について、対応する第14～第17の実施形態を説明する。

【0380】(第14の実施の形態)本実施形態は改竄を防止できる電子文書の変更システム及び方法に関するものである。

【0381】図37は本発明の第14の実施形態に係る文書変更を含んだ電子文書の改竄防止システムに適用される文書変更認証システムのハードウェア構成例を示すブロック図である。

【0382】文書変更認証システム1103は、計算機1110に、表示装置1111、入力装置1112、印刷装置1113、外部記憶装置1114、指紋読み取り機1064、スキャナ1115が接続されてなっている。

【0383】この文書変更認証システム1103の上記ハードウェア構成は、図2に示す文書認証システム101と同様なものであり、ここでは説明を省略する。すなわち、計算機1110、表示装置1111、入力装置1112、印刷装置1113、外部記憶装置1114、指紋読み取り機1064、スキャナ1115が、それぞれ計算機110、表示装置111、入力装置112、印刷装置113、外部記憶装置114、指紋読み取り機64、スキャナ115に対応する。

【0384】また、計算機1110内の構成についても同様であり、文書変更認証システム1103の各構成要素1116～1133が、文書認証システム101の各構成要素116～133に対応している。

【0385】ただし、ハードディスク装置1128やRAM1119等に格納されるソフトウェア的要素のうち、文書変更認証システム1103に対応する部分は本実施形態独自のものとなる。すなわちプログラム格納部1130は文書変更認証システム1101を実現するプログラム等を格納し、また、RAM1119は、文書変更認証プログラム1133を格納する。なお、第1実施形態と同様に、この文書変更認証プログラム1133は、ハードディスク装置1128のプログラム格納部1130から呼び出され、RAM1119内に格納される。

【0386】また、CPU1117は、RAM1119内の文書変更認証プログラム1133に従って各部を制御し、文書変更認証システム1103を実現する。

【0387】本実施形態及び以下の各実施形態における処理説明図や流れ図などに表現される各手段(各処理)あるいは図示しない各手段(各処理)は、主として文書変更認証プログラム1133に従うCPU1117の動作による機能実現手段である。

【0388】次に外部認証システムのハードウェア構成

について説明する。

【0389】図38は本実施形態の文書変更を含んだ電子文書の改竄防止システムに適用される外部認証システムのハードウェア構成例を示すブロック図であり、図37と同一部分には同一符号を付してその説明を省略する。

【0390】外部認証システム1102は、文書変更認証システム1103と同様な計算機システムから構成される。文書変更認証システム1103との相違点は、ハードディスク装置1128のプログラム格納部に格納される動作プログラムである。この動作プログラムが呼び出され、RAM1119内に外部認証プログラム1134として格納される。CPU1117は、この外部認証プログラムに従って各部を制御し、外部認証システム1102が実現される。また、ソフトウェア資源(特に外部認証プログラム1134)とハードウェア資源とが結合して機能実現手段が構成される点も文書変更認証システム1103の場合と同様である。

【0391】次に図39及び図40を用いて文書変更を含んだ電子文書の改竄防止システムの各構成について説明する。

【0392】図39及び図40は本実施形態の文書変更を含んだ電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図である。

【0393】この文書変更を含んだ電子文書の改竄防止システムは文書変更認証システム1103と外部認証システム1102とから構成されている。

【0394】まず図39の構成を説明する。

【0395】文書変更認証システム1103は、分離手段1005と、変更者#nの変更及び認証手段1006と、結合手段1009とから構成され、変更履歴付電子文書1001から変更履歴付電子文書1011を生成するようになっている。

【0396】ここで変更履歴付電子文書1001は、過去に変更があった電子文書あるいは過去に変更はないがこれから変更を施す電子文書であって、認証付き原電子文書1002と、1回目変更からn-1回目変更までの認証付き変更箇所データ1003と、n-1回目の認証付き変更電子文書1004とから構成されている。

【0397】分離手段1005は、変更履歴付電子文書1001を各構成要素に分離する。

【0398】変更者#nの変更及び認証手段1006は、n-1回目の認証付き変更電子文書1004を外部認証システム102に送出し、その応答結果に基づき、変更者#nによるn回目変更箇所1007、変更者#nによるn回目変更電子文書1008を出力する。

【0399】結合手段1009は、認証付き原電子文書1002と、1回目変更からn-1回目変更までの認証付き変更箇所データ1003と、変更者#nによるn回目変更箇所1007と、変更者#nによるn回目変更電子文書1

008とを結合して変更履歴付電子文書1011を生成する。ここで、変更履歴付電子文書1011は、認証付き原電子文書1002と、1回目からn回目までの変更箇所1010と、n回目変更電子文書1008とから構成される。

【0400】次に、図40を用いて変更者#nの変更及び認証手段1006の詳細構成及び外部認証システム1102の概略構成を説明する。

【0401】変更者#nの変更及び認証手段1006は、文書変更手段1021と、差分抽出手段1023と、変更者認証手段1025A、1025Bと、結合手段1028とを備えている。

【0402】文書変更手段1021は、変更電子文書1020を変更者#nによる変更電子文書1022に変換する。差分抽出手段1023は、変更電子文書1020と変更者#nによる変更電子文書1022との差分を抽出し、この差分データから構成されるn回目変更箇所1024を生成する。

【0403】変更者認証手段1025A、1025Bは、それぞれ変更者の認証データで変更電子文書1022、変更箇所1024を認証し、変更者認証データ1026A、変更者差分認証データ1026Bを出力する。

【0404】結合手段1028は、認証データ1027と変更者認証データ1026Aとを結合し、結合認証データ1029を出力する。

【0405】特に図示しないが、変更者#nの変更及び認証手段1006は、さらに、n-1回目の認証付き変更電子文書1004から変更電子文書1020及び認証データ1027を取り出す手段と、変更箇所1024と認証データ1032Bを結合して変更箇所1007を生成する手段と、変更電子文書1022と認証データ1032Aとを結合して変更電子文書8を生成する手段とを備えている。

【0406】一方、外部認証システム102は、認証データ1029に対し、外部認証機関による認証を行って認証データ1031Aを生成する外部認証手段1030Aと、変更者差分認証データ1026Bに対し、外部認証機関による認証を行って認証データ1031Bを生成する外部認証手段1030Bとを備えている。

【0407】なお、認証データ1029及び変更者差分認証データ1026Bは、文書変更認証システム1103から外部認証システム1102に送信され、その認証結果1031A、1031Bが外部認証システム1102から返信されるようになっている。

【0408】次に、図41を用いて、変更者#nの変更及び認証手段1006の変更者認証手段1025Aについて説明する。

【0409】図41は変更者#nの変更及び認証手段における変更者認証手段の構成を示す図である。

【0410】変更認証手段1025Aは、変更者#nの秘

密鍵1025A-3及び見出し1026A-Hを保持するとともに、特徴抽出手段1025A-1及び暗号化手段1025A-4を備えている。

【0411】特徴抽出手段1025A-1は、変更電子文書22から特徴データ1025A-2を抽出して暗号化手段1025A-4に引き渡す。暗号化手段1025A-4は、特徴データ1025A-2を変更者#nの秘密鍵1025A-3で暗号化して暗号データ1026A-Dを生成する。

【0412】変更認証手段1025Aは、暗号データ1026A-Dに見出し1026A-Hを付加して、変更者の認証データ1026Aを生成する。

【0413】なお、変更者認証手段1025Bについては特に図示しないが、変更者認証手段1025Aと同様に構成される。

【0414】図42は外部認証システムにおける外部認証手段の構成を示す図である。

【0415】外部認証手段1030Aは、認証実行IDを含む外部認証データ1030A-A及び外部認証機関の秘密鍵1030A-2を保持するとともに、結合手段1030A及び暗号化手段1030A-3を備えている。

【0416】文書変更認証システム1103から送信される結合認証データ1029は、見出し1026A-H及び暗号データ1026A-Dからなる変更者の認証データ1026Aと、認証データ1027とから構成されている。この結合認証データ1029は、外部認証手段1030Aにて、見出し1031A-Hと、暗号データ1026A-D及び認証データ1027とに分離される。

【0417】暗号化手段1030Aは、外部認証データ1030A-Aと、暗号データ1026A-D及び認証データ1027とを結合し、暗号化手段1030A-3は、この結合結果を秘密鍵1030A-2で暗号化する。

【0418】外部認証手段1030Aにより最終的に生成される外部認証機関の認証データ1031Aは、見出し1031A-Hと、暗号化手段1030A-3により暗号化された暗号データ1031A-Dからなる。

【0419】なお、外部認証手段1030Bについては特に図示及び説明しないが、これは外部認証手段1030AにおけるAとBとを読み替えたものと同じである。

【0420】次に、以上のように構成された本発明の実施の形態に係る電子文書の改竄防止システムの動作について図39～図43を用いて説明する。

【0421】図43は本実施形態の電子文書の改竄防止システムの動作を示す流れ図である。

【0422】まず、文書変更認証システム1103において、変更履歴付電子文書1001の読み込みが行われる(SS1)。

【0423】次に、分離手段1005によって、変更履歴付原電子文書1002、変更履歴付n-1回目までの変更箇所1003及び変更履歴付n-1回目的変更電子文書1004に分離される（SS2）。

【0424】次のステップSS3からSS7までの処理は変更及び認証手段1006によって行われる。すなわち、図39及び図40に示すように、変更者#n(以下、複数存在し得る同種類の構成やデータには、場合により#1、#2、..あるいは第1の、第2の、..と記して区別する)が使用する変更及び認証手段6により、取り出されたn-1回目的認証付き変更電子文書1004が変更され及び変更者#nの認証が行われ、変更者#nの認証データが外部認証システム1102に送信される。

【0425】具体的にはまず、n-1回目的認証付き変更電子文書1004から、n-1回目変更電子文書1020が取り出される。さらに、変更者#nの入力操作で変更手段1021により、n-1回目の変更電子文書1020が変更され、n回目の変更電子文書1022が生成される（SS3）。

【0426】次に、差分抽出手段1023により、n-1回目的変更電子文書1020とn回目の変更電子文書1022と差分の抽出が行なわれ、n回目変更箇所1024の差分データが抽出される（SS4、図40）。

【0427】この処理（SS4）は、次のようにしてなされる。すなわち各電子文書は詰まる所0と1から構成されるバイナリデータである。差分抽出手段1023は、これらバイナリデータの差分を抽出して、n回目変更箇所データ1024を出力する。これによりn回目変更箇所データ1024には、n-1回目変更電子文書1020とn回目変更電子文書1022の間でどの場所でどのデータが削除されたか、どの場所でどのデータが挿入されたか、どの場所でどのデータが入れ替えられたかの情報が保存される。

【0428】次に、変更者#nによる文書変更完了後の認証行われ、n回目変更電子文書1022とn回目変更箇所1024からそれぞれn回目変更電子文書の変更者認証データ1026Aとn回目変更箇所の変更者認証データ1026Bが生成される（SS5、図40）。

【0429】すなわちn回目変更電子文書1022が変更者認証手段1025Aに与えられ、n回目変更者認証データ1026Aが生成される。このためにまず、特徴抽出手段1025A-1によってn回目変更変更電子文書1022の特徴データ1025A-2が抽出される（図41）。この特徴データ1025A-2はn回目変更変更電子文書1022のどの1ビットが変化してもその値が異なった値となる様な電子文書自体の特徴を示すデータである。一方、見出し1026A-Hは、特徴データ1025A-2がn回目変更変更電子文書1022に属するデータである事をわかるようにする為に追加されるデータである。

【0430】次に、特徴データ1025A-2は、変更者#nの秘密鍵1025A-3を使用して暗号化手段1025A-4で暗号化され、暗号データ1026A-Dとして出力される。変更者#nの秘密鍵1025A-3は、文字通り、変更者#n以外には知らせない様にした鍵で、変更者#nの公開鍵と対を成すものである。見出し1026A-Hと暗号データ1026A-Dとは対応しており、まとめて変更者認証データ1026Aとして出力される。

【0431】同様に、変更者認証手段1025Bによってn回目変更箇所データ1024から特徴が抽出され、n回目変更者差分認証データ1026Bが生成される。

【0432】次に、n-1回目的認証付き変更電子文書1004から取り出したn-1回目的変更電子文書認証データ1027と、n回目の変更電子文書の変更者認証データ1026Aと結合手段28によりが結合され、n回目の結合認証データ1029が生成される（SS6、図40）。

【0433】次に、n回目の結合認証データ1029とn回目変更箇所の変更者認証データ1026Bとが文書変更認証システム1103の通信装置1129を介してネットワーク1100を通り外部認証システム1102に送信される（SS7）。

【0434】次のステップSS8からSS10までの処理は外部認証システム1102において行われる。

【0435】まず、外部認証システム1102は文書変更認証システム1103から送られたn回目変更文書の変更者結合認証データ1029とn回目変更者差分認証データ1026Bを受信する（SS8）。

【0436】次に、外部認証システム1102において、送られたn回目の結合認証データ1029とn回目変更箇所の変更者認証データ1026Bとがそれぞれ外部認証手段1030A、1030Bにより認証され、それぞれ認証データ1031A、1031Bが生成される（SS9、図40）。以下にこの処理を説明する。

【0437】このためにまず、外部認証手段1030Aによって、n回目変更文書の変更者結合認証データ1029から見出し1031A-Hが取り出される。引き続いて、残りの暗号データ/認証データ1026A-D/1027が結合手段1030A-1に与えられる（図42）。

【0438】この暗号データ/認証データ1026A-D/1027に、外部認証機関の外部認証データ1030A-A（認証実行ID）が結合手段1030A-1により結合される。なお、この認証実行識別情報としての認証実行IDは原則として認証毎に異なるものであり、どの認証に対してどの認証実行IDを付与したかは、外部認証機関1099に保存される。

【0439】次に、この結合データが、外部認証機関の

秘密鍵1030A-2を用いて暗号化手段1030A-3により暗号化され、暗号データ1031A-Dが生成される。

【0440】ここで、外部認証データ1030A-Aは文書変更認証システム1103が認証を要求してきたデータに対して第三者である外部認証機関が認証した事を示す情報であり、認証した日付データが含まれる。見出し1031A-Hと暗号データ1031A-Dは、データの関係付けが行われ、n回目変更電子文書認証データ1031Aとして出力される。

【0441】同様に、変更者差分認証データ1026Bも外部認証手段1030Bによって外部認証が与えられ、n回目差分認証データ1031Bとして出力される。この場合の外部認証手段1030Bの処理については、図42のAをBと読み替えて説明を行なう。

【0442】すなわち外部認証手段1030Bでは、n回目変更文書の変更者結合認証データ1029を受け取る代わりに、n回目変更者差分認証データ1026Bからデータを受け取ると、見出し1031B-Hを取り出して、残りの暗号データ1026B-Dが結合手段1030B-1に与えられる。前記暗号データ1026B-Dに外部認証機関の外部認証データ1030B-Aが結合手段1030B-1により結合され、外部認証機関の秘密鍵1030B-2を用いて暗号化手段1030B-3により暗号化され暗号データ1031B-Dを生成する。ここで、外部認証データ1030B-Aは文書変更認証システム1103が認証を要求してきたデータに対して第三者である外部認証機関が認証した事を示す情報であり、認証した日付データが含まれる。見出し1031B-Hと暗号データ1031B-Dはn回目差分認証データ1031Bとしてデータの関係付けが行われる。

【0443】こうして生成されたn回目変更電子文書認証データ1031A及びn回目差分認証データ1031Bは、外部認証システム1102の通信装置1129を介してネットワーク1100を通り文書変更認証システム1103に送信される(SS10)。

【0444】文書変更認証システム1103においては、外部認証システム1102から送られたデータを認証データ1032A、1032Bとして受信し、この受信データを変更及び認証手段1006に与える(SS11)。

【0445】次に、変更及び認証手段1006において、n回目変更電子文書認証データ1031Aはn回目変更電子文書1022との関係付けが行われ、n回目の認証付き変更電子文書1008が生成され出力される。同様に、n回目差分認証データ1031Bはn回目変更箇所データ1024との関係付けが行われ、n回目の認証付き差分認証データ1007が生成され出力される(SS12、図40)。

【0446】次に、変更箇所データ1007は、結合手

段1009によって、1回目変更からn-1回目変更までの認証付き変更箇所データ1003と結合され、各々関係付けのなされた1回目からn回目までの認証付き変更箇所データ1010となる。さらに、結合手段1009により、認証付き原電子文書1002、1回目からn回目までの認証付き変更箇所データ1010およびn回目認証付き変更電子文書1008が関係付けられたn回目変更履歴付電子文書1011が生成される(SS13、図39)。

10 【0447】なお、n+1の変更を実施する時には、変更履歴付電子文書1001をn回目の変更履歴付き電子文書とすると、n+1回目の変更履歴付き電子文書が変更履歴付電子文書1011として得られる。

【0448】上述したように、本発明の実施の形態に係る変更電子文書の改竄防止システム及び方法は、変更者により電子署名された変更文書を外部認証機関が認証する手順を踏んで追加的な認証を行うようにしたので、外部認証機関の認証日付にはまさしく変更者が変更文書を作成していた事が証明される。また、電子署名が無い場合であっても文書変更者本人の秘密鍵で特徴データの暗号化がなされ、これに対応する公開鍵で復号化される事になるので、何れにしても文書変更者の変更になる文書である事が認証される。

【0449】また、変更文書本体の改竄を行なうと改竄後の文書から抽出されるべき特徴データが変化し、先に認証用に抽出された特徴データ1025A-2と異なるものになる事によって、変更文書本体の改竄の事実が検出できる。一方先に認証用に抽出された特徴データ1025A-2は外部認証機関の認証データ1030A-Aとともに認証機関の秘密鍵1030A-2で暗号化されているので、認証付き変更電子文書1008に付されている認証データ1032Aの改竄は不可能である。従って、たとえ本人であっても外部認証後には文書改竄が不可能になる。

【0450】これにより裁判の場で文書の正当性が証明できる、証拠能力のある変更電子文書が生成できるため、従来紙で保存していた重要文書や、証拠書類を電子化する事が可能となる。また、従来の紙の文書でも改竄の有無を判定するには高度な技術が必要とされたが、本発明になる電子文書の改竄防止システムでは電子的な手順を踏むだけで改竄の有無を確認できるので、改竄の有無を容易に証明できる。

【0451】さらに電子化により保管場所が削減できると共に、遠隔地への文書伝送が瞬時に行なえる様になり、コンピュータによる検索が行なえるようになる。こうして、商取引の信用向上、取り引きの迅速化を図る事ができる。

【0452】また、本実施形態の変更文書改竄防止システムでは、文書変更認証システム1103や外部認証システム1102に於いて伝送データの暗号化が行われる

ので、ネットワーク1100として公衆回線を用いても安全である。

【0453】さらに、本実施形態の変更文書改竄防止システムでは、文書変更認証システム1103と外部認証システム1102との間でやり取りされるデータは文書データではなく、文書データの特徴(差分データ等)であるので、文書データそのものの内容はネットワーク1100や外部認証システム1102に流す必要が無く、文書データの秘密を保つ事ができる。

【0454】さらに、外部認証機関が認証した外部認証データを元の変更電子文書と変更箇所と結合して認証付きの変更履歴付文書1011の形で管理するようにしたので、電子文書を保存する時の扱いが楽になる。

【0455】(第15の実施の形態)本実施形態では、第14の実施形態で認証した認証付き変更電子文書1011が真正なものである事を確認し、また外部認証機関の付した認証日付などの認証情報を取り出すシステムについて説明する。

【0456】この変更電子文書の改竄防止システムは、図36に示した認証文書確認システム1104として構成されるものである。

【0457】図44は本発明の第15の実施の形態に係る変更電子文書の改竄防止システムに適用される認証文書確認システムのハードウェア構成例を示すブロック図であり、図37と同一部分には同一符号を付してその説明を省略する。

【0458】認証文書確認システム1104は、文書変更認証システム1103と同様な計算機システムから構成される。文書変更認証システム1104との相違点は、ハードディスク装置1128のプログラム格納部1130に格納される動作プログラムである。この動作プログラムが呼び出され、RAM1119内に認証文書確認プログラム1135として格納される。CPU1117は、この認証文書確認プログラム1135に従って各部を制御し、認証文書確認システム1104が実現される。また、ソフトウェア資源とハードウェア資源とが結合して機能実現手段が構成される点も文書変更認証システム1103の場合と同様である。

【0459】次に図45～図47を用いて電子文書の改竄防止システムの機能構成について説明する。

【0460】図45は本実施形態の変更電子文書の改竄防止システムに適用される認証文書確認システムの機能構成ならびに処理流れの一例を示す図であり、図39と同一部分には同一符号を付して説明を省略する。

【0461】同図において、認証確認の対象となる変更電子文書1011Bは、原電子文書1002Bと、変更電子文書1008Bと、1回目からn回目までの変更箇所1007B#1～1007B#n-1及び1007Bとからなり、これは第14の実施形態における変更電子文書1011に対応している。

【0462】一方、認証文書確認システム1104には、n回目の認証確認手段1040と、n-1回目の認証確認手段1040#n-1と、日付確認手段1041、1041#n-1と、同一性判定手段1042、1042#n-1とが設けられる。さらに、認証文書確認システム1104には、繰返し部分となる認証確認手段1040と同様な認証確認手段1043と、第1～第13の実施形態におけるものと同様な認証確認手段1044、日付確認手段1045及び同一性判定手段1046とが設けられている。

【0463】また、認証文書確認システム1104には、変更履歴付電子文書1011Bから認証付き原電子文書1002Bと、1回目変更からn回目変更までの認証付き変更箇所データ1007B#1、1007B#2、…1007B#n-1、1007Bと、n回目の認証付き変更電子文書1008Bとを取り出し、認証データと文書データと変更箇所データとに分解する手段(図示せず)が設けられている。

【0464】次に図46及び図47を用いて認証文書確認システム1104を構成する認証確認手段の各機能構成について説明する。

【0465】図46は認証確認手段1040の詳細構成を示す図であり、図47は認証確認手段1040#n-1の詳細構成を示す図である。

【0466】認証確認手段1040は、n回目の認証付き変更電子文書1008Bの認証を確認する認証確認手段1040Aと、n回目の認証付き変更箇所1007Bの認証を確認する認証確認手段1040Bとから構成される。

【0467】認証確認手段1040Aにおいては、認証データ1401A、外部認証機関1099の公開鍵1402A、見出しを含む変更者結合認証データ1404A、変更者認証データ1406A、以前の認証データ1407A、変更者の公開鍵1408A、特徴データ1410A及び特徴データ1412Aが保持されている。また、復号化手段1403A、分離手段1405A、復号化手段1409A、特徴抽出手段1411A及び照合手段1413Aが設けられている。

【0468】ここで、見出しを含む変更者結合認証データ1404Aは、見出し1401A-Hと暗号データ1401A-Dから構成される。また、見出しを含む変更者結合認証データ1404Aは、見出し1404A-Hと変更者結合認証データ1404A-Dとから構成され、変更者結合認証データ1404A-Dはさらに変更者結合認証データ1404A-D1と外部認証機関1099の認証データ1404A-D2とから構成される。以前の認証データ1407Aは見出しと認証データ本体とから構成される。

【0469】一方、認証確認手段1040Bにおいて、認証データ1401B、外部認証機関1099の公

開鍵1402B、見出しを含む変更者認証データ1404B、変更者の公開鍵1408B、特徴データ1410B、特徴データ1412Bが保持されている。また、復号化手段1403B、復号化手段1409B、特徴抽出手段1411B、照合手段1413Bが設けられている。

【0470】ここで、見出しを含む変更者認証データ1401Bは見出し1401B-Hと暗号データ1401B-Dから構成される。見出しを含む変更者認証データ1404Bは見出し1404B-Hと変更者認証データ1404B-Dとから構成され、変更者認証データ1404B-Dはさらに変更者認証データ1404B-D1と外部認証機関1099の認証データ1404B-D2とから構成される。

【0471】次に図47を用いて認証確認手段1040 #n-1を説明する。

【0472】認証確認手段1040 #n-1は、n-1回の認証データ1027の認証を確認する認証確認手段1040Aと、n-1回目の認証付き変更箇所1007B #n-1の認証を確認する認証確認手段1040Bとから構成される。

【0473】ここで、図47における認証確認手段1040A及び1040Bと図46における認証確認手段1040A及び1040Bとは同一の手段を使用するが、n-1回以前の認証データ1027の認証確認で使用しない機能は図示を省略している。

【0474】次に、以上のように構成された本発明の実施の形態に係る電子文書の改竄防止システムの動作について図45～図50を用いて説明する。

【0475】この認証文書確認システム1104においては、変更履歴付電子文書1011B内のn回目の認証付き変更電子文書1008Bからスタートしてn回目の側から原文書の方に向かって順次認証の確認が繰返され、原文書と最終文書、および全ての変更箇所の電子文書の同一性確認が行われる。また、認証データから取り出された外部認証データから外部認証機関1099による認証の事実及びその認証日付1045、1041 #1、1041 #2、…1041 #n-1、1041が確認される。

【0476】図48は本実施形態の電子文書の改竄防止システムの動作を示す流れ図である。

【0477】同図においてまず、外部記憶装置1114、ハードディスク装置1128から、あるいはネットワーク1100を介して変更履歴付電子文書1011Bが読み込まれる(TT1)。この変更履歴付電子文書1011Bからは、認証付き原電子文書1002Bと、1回目変更からn回目変更までの認証付き変更箇所データ1007B #1、1007B #2、…1007B #n-1、1007Bと、n回目の認証付き変更電子文書1008Bとが取り出され、さらに認証データと文書データ、変

更箇所データに分解される(TT2)。

【0478】次に、文書変更回数Nが最終の変更回数n回に設定され、認証確認初回フラグが設定される(TT3)。

【0479】ここで、初回の認証確認かどうか判断される(TT5)。初回の場合にはN回目変更文書データ1008Bの認証データ、N回目変更文書1008Bの文書データ、N回目変更箇所1007Bの変更認証データ、及びN回目変更箇所1007Bの変更箇所データが認証確認手段1040に読み込まれる(TT6)。

【0480】続いて認証確認手段1040により認証確認が実行され、認証データ1027が出力され、少なくとも外部認証機関の日付と認証実行IDを含んだ日付認証データ1041が生成される(TT8)。

【0481】一方、ステップTT5で初回でない場合には、Nの数に応じてn-1回目変更箇所1007B #n-1から1回目変更箇所1007B #1までのどれかが認証確認手段1040に読み込まれる(TT7)。

【0482】続いて認証確認手段1040 #n-1、1040 #n-2…により認証確認が実行され、認証データ1027が出力され、日付認証データ1041 #n-1、1041 #n-2…が生成される(TT8)。ここで認証確認手段1041 #n-1、1041 #n-2…は同じ認証確認手段が繰り返し呼び出される。

【0483】ここで、n回目、n-1回目及びn-2回目から1回目におけるステップTT8の認定内容について簡単に説明する。

【0484】すなわちまず、n回目の認証付き変更電子文書1008B及びn回目の認証付き変更箇所1007Bの認証確認が認証確認手段1040により行われる。これにより、n-1回目までの認証データ1027が出力され、外部認証機関の認証日付1041が出力される。さらに、n回目変更電子文書1008Bとn回目認証付き変更箇所1007Bが、変更履歴付電子文書1011のn回目変更電子文書1008とn回目認証付き変更箇所1007と同一であるか否かの同一性判定1042が行われる。

【0485】また、n-1回目の認証付き変更箇所1007B #n-1の認証確認は、認証確認手段1040 #n-1により行われる。すなわち、n-2回目までの認証データ1027 #n-1が出力され、外部認証機関の認証日付1041 #n-1が出力される。さらに、n-1回目認証付き変更箇所1007B #n-1が変更履歴付電子文書1011のn-1回目認証付き変更箇所1007 #n-1と同一であるか否かの同一性判定1042 #n-1が行われる。

【0486】また、同様に認証確認手段1043により、n-2回目から1回目の認証付き変更箇所1007B #1から1007B #n-2に基づき、それぞれの回の認証データ及び外部認証機関の認証日付が出力される。さらに、認証付き変更箇所1007B #1…1007B #n-2が変更

履歴付電子文書1011の認証付き変更箇所1007#1
…1007#n-2と同一であるか否かの同一性判定が行わ
れる。

【0487】以上の何れかの認証確認(TT8)が実行
された後、認証実行IDの不一致または同一性判定手段
1042の判定が否の場合(TT9)は、N回目文書の
不一致が表示装置1111に表示されて終了する。な
お、外部記憶装置1114に出力したり、ハードディ
スク装置1128に出力したり、ネットワーク1100に
出力したりして終了してもよい(TT10)。

【0488】一方、認証実行IDが一致しかつ同一性判
定手段1042の判定が真の場合(TT9)には、認証
確認初回フラグがクリアされ、変更回数Nを1減じる
(TT11)。

【0489】次に変更回数Nが1かどうか判定され
(TT12)、Nが1より大きい場合にはステップTT
4に戻り、初回の認証確認かどうか判断されて(TT
5)、ステップTT5～ステップTT12が繰り返され
る。

【0490】一方、変更回数Nが1の場合には(TT1
2)、認証付き原電子文書1002Bの認証データと文
書データが認証確認手段1044に読み込まれる(TT
13)。なお、ここで与えられる認証データは認証確
認手段1043から出力されるものであり、文書データ
は、認証付き原電子文書1002Bから認証部分を除い
たものである。

【0491】続いて、認証確認手段1044により認証
確認が実行され、原文書の外部認証機関の日付認証デ
ータ1045が出力され、原電子文書1002Bと原電子
文書1002とが同一であるか否かの同一性判定104
6が行われる(TT14)。なお、認証確認手段104
4により認証確認処理は、先の実施形態におけるもの
と同様であるので説明を省略する。

【0492】ここで同一性判定手段1046の判定が否
の場合(TT15)には、原電子文書1002Bが不
一致である旨が表示装置1111に表示されて終了する。
なお、外部記憶装置1114に出力したり、ハードディ
スク装置1128に出力したり、ネットワーク1100
に出力したりして終了してもよい(TT16)。

【0493】一方、同一性判定手段1046の判定が真
の場合(TT15)には、文書一致である旨と、原電子
文書の作成日付からn回目変更文書までの変更日付とが
表示装置1111に表示されて終了する。また、外部記
憶装置1114に出力したり、ハードディスク装置11
28に出力したり、ネットワーク1100に出力したり
して終了してもよい(TT17)。なお、認証日付は、
認証確認手段1040A、Bで得られた両者を表示して
もよいし、片方を表示してもよい。また、両者の日付が
一致している事を判定するようにしてもよい。

【0494】また、ステップTT17では原文書の作成

者、各回の変更者の名前などを出力する様にしてもよ
い。

【0495】以上が本実施形態における認証文書確認シ
ステム1104の全体的な処理流れである。ここで次に
図48におけるステップTT8の処理、つまり、認証確
認手段1040及び1040#n-1の処理についてより具
体的に説明する。

【0496】図49は本実施形態の認証確認システムに
おける認証確認手段1040Aの処理を示す流れ図であ
る。

【0497】同図は、認証確認手段1040及び104
0#n-1の処理の双方を示しているが、ここでは認証確
認手段1040の処理の場合を例にとって説明する。

【0498】まず、認証確認手段1040Aにn回目の
認証付き変更電子文書1008Bから認証データの部分
が入力される。この認証データ1401Aは、n回目の
認証付き変更電子文書1008Bである事を分る様に
した見出し1401A-Hと、暗号データ1401A-Dとに
分離される(T801、図46)。なお、n-1…
1回目変更の場合にあっては、後述するステップT81
1及びT812にて出力される以前の認証データ及び見
出しが上記各データとして用いられる。

【0499】このうち、暗号データ1401A-Dは外
部認証機関1099の公開鍵1402Aを用いた復号化
手段1403Aにより復号され、変更者結合認証データ
1404A-Dが出力される(T802、図46)。こ
のとき、変更者結合認証データ1404A-Dと見出し
1401A-Hとは関係付けられ、認証データ1404
Aとなる(T803、図46)。

【0500】次に、変更者結合認証データ1404A-D
にある外部認証データ1404A-D2から少なくとも
日付データと認証実行IDが取り出され、日付認証手
段1041に与えられる(T804、図46)。

【0501】一方、変更者結合認証データ1404A-D
の中の変更者認証データ1404A-D1は分離手段
1405Aに与えられ、変更者認証データ1406Aと
以前の認証データ1407A分離される(T805、図
46)。ここで、以前の認証データ1407Aは原文書
の認証からn-1回までの変更文書の認証を含むデータ
である。以前の認証データ1407Aは認証確認手段10
40#n-1に与える認証データ1027として出力され
る。

【0502】次に、認証確認初回フラグが確認され、初
回の場合にはステップT807が実行され、初回でない
場合には、ステップT810に移動する(T806)。

【0503】ステップT807が実行される場合には、
復号化手段1409Aにより、変更者認証データ140
6Aが変更者のn回目の公開鍵1408Aで復号化されn
回目の特徴データ1410Aが生成される(T807、
図46)。

10

20

30

40

50

【0504】一方、最終回（ n 回目）変更にあつては変更電子文書データ1008Bから文書データの部分を受け取り、文書データの特徴が特徴抽出手段1411Aにより抽出され、特徴データ1412Aが出力される（T808、図46）。なお、 $n-1 \cdots 1$ 回目変更にあつては認証データ1027、1027# $n-1$ 、 \cdots 1027#2から特徴データが抽出される。

【0505】次に、復号化された特徴データ1410Aと認証確認の為に特徴抽出された特徴データ1412Aとが照合手段1413Aにより照合され、その結果が同一性判定手段1042に出力される（T809）。同一性判定手段1042にて照合結果が一致と判定された場合には、変更電子文書1008と変更電子文書1008Bとが一致していると証明される。

【0506】さらに、認証確認手段1040Aからは、以前の認証データ1407Aが認証データ1027として出力され（T811）、今回の変更に関する見出し1404A-Hが出力される（T812）。これらは、 $n-1 \cdots 1$ 回目変更の認証に用いられることになる。

【0507】次に認証確認手段1040のうち、認証確認手段1040B部分の処理を説明する。

【0508】図50は本実施形態の認証確認システムにおける認証確認手段1040Bの処理を示す流れ図である。

【0509】同図は、認証確認手段1040及び1040# $n-1$ の処理の双方を示しているが、ここでは認証確認手段1040の処理の場合を例にとって説明する。

【0510】まず、 n 回目の認証付き変更箇所1007Bから認証データの部分が認証確認手段1040Bに入力される。この入力された認証データ1401Bは、 n 回目の認証付き変更箇所1007Bである事を分かる様にした見出し1401B-Hと暗号データ1401B-Dとに分離される（T821、図46）。

【0511】次に、暗号データ1401B-Dは、復号化手段1403Bに与えられ、外部認証機関1099の公開鍵1402Bが用いられて復号され、変更者認証データ1404B-Dが生成される（T822、図46）。ここで公開鍵1402Bは公開鍵1402Aと同じ内容のものである。

【0512】また、変更者認証データ1404B-Dと見出し1404B-Hとが関係付けられ、認証データ1404Bとされる（T823、図46）。

【0513】変更者認証データ1404B-Dにある外部認証データ1404B-D2から少なくとも外部認証機関1099の日付データと認証実行IDとが取り出され、日付認証手段1041に与えられる（T824、図46）。

【0514】一方、変更者認証データ1404B-Dの中の変更者認証データ1404B-D1は、復号化手段1409Bに与えられる。復号化手段1409Bにおい

ては、 n 回目の変更者の公開鍵1408Bが使用されて、変更者認証データ1404B-D1が復号化されて n 回目の変更箇所の特徴データ1401Bが取り出される（T827、図46）。ここで公開鍵1408Bは公開鍵1408Aと同じ内容のものである。

【0515】一方、最終回（ n 回目）変更にあつては変更箇所データ1007Bから変更箇所データの部分を受け取り、変更箇所データの特徴が特徴抽出手段1411Bにより抽出され、特徴データ1412Bが出力される（T828、図46）。なお、 $n-1 \cdots 1$ 回目変更にあつては変更箇所データ1007、1007# $n-1$ 、 \cdots 1007#2から特徴データが抽出される。

【0516】次に、復号化された特徴データ1410Bと認証確認の為に特徴抽出された特徴データ1412Bとが照合手段1413Bにより照合され、その結果が同一性判定手段1042に出力される（T829）。同一性判定手段1042にて照合結果が一致と判定された場合には、変更箇所1007と変更箇所1007Bとが一致していると証明される。なお、より具体的には、認証確認手段1040A、Bにおける両方の照合手段の結果が両方とも同一の判定である時に $n-1$ 回目から n 回目の文書変更での文書改竄が無い事が証明されるものである。

【0517】さらに、認証確認手段1040Bからは、今回の変更に関する見出し1404B-Hが出力される（T832）。

【0518】以上は、主に認証確認手段1040による認証確認処理（図48：ステップT8）を説明した。しかし、認証確認手段1040# $n-1$ 及び1043による認証確認処理ではこれと多少異なる部分があるので、その部分について図47、図48及び図49を用いて説明する。

【0519】まずは、認証確認手段1040# $n-1$ による処理について説明する。

【0520】認証確認手段1040から出力された $n-1$ 回の認証データ1027が、図47における認証データ1401Aとして認証確認手段1040# $n-1$ の認証確認手段1040Aに与えられる。同一性判定手段1042# $n-1$ に与えられる比較照合結果がただ一つである点を除けば、以下の処理は、認証確認手段1040の場合と同様である。なお、図47における認証データ1407Aは、認証データ1027として次の認証確認手段1043に与えられる。

【0521】また、認証確認手段1043では、認証確認手段1040# $n-1$ と同様な処理が繰り返され、 $n-2$ 回目から1回目までの認証確認が行われる。

【0522】上述したように、本発明の実施の形態に係る変更電子文書の改竄防止システム及び方法は、原文及び変更#1から変更# n までの暗号化特徴データの付加と、原文作成者及び変更者#1から# n までの本人認証及び外部認証機関の認証とがなされた変更電子文書から、 n から1

に向かって順次外部認証機関の認証データを取り出し、また付加されている文書データの特徴データ及び変更箇所の特徴データと確認対象の電子文書本体からの特徴データ及び変更箇所の特徴データとを文書変更者#nから#1までの公開鍵を用いて照合するようにしたので、変更毎の外部認証機関の認証日付には、まさしく変更者#1から#nが文書変更を行っていた事を証明することができる。

【0523】なお、電子文書本体の改竄を行なうと、電子文書1008Bから抽出される特徴データ1411Aが変化することにより、一方、特徴データ1410Aは外部認証機関1099によって改竄を防止されることによって、変更者本人であっても外部認証後には文書改竄が不可能になる。

【0524】また、変更者#nが電子文書1008Bの差し替えを行なうと、外部認証機関1099が外部認証手段1030A及び外部認証手段1030Bにより付加した認証実行IDデータが変更若しくは消失していることが日付認証1041で発見される。したがって、当該差し替えは不可能である。また、原文1002Bの認証は認証データ1027#1を使用するので、原文1002B自体の改竄、差し替えも不可能である。

【0525】このように変更履歴付電子文書1011Bは変更者自身のみならず、外部認証機関、その他何人足りとも改竄をする事はできない。

【0526】これにより裁判の場で変更文書の原文から変更履歴全ての段階に於いて文書の正当性が証明でき、製造記録や検査記録等の同じ利害関係を持った複数人の変更記録に対しても証拠書類の電子化が可能となる。

【0527】また、外部認証機関の認証は特徴データに対して行なわれるので、外部に対して秘密を保持する事が必要な文書に対してもネットワーク1100として公衆回線を使用しても安全である。

【0528】さらに、外部認証機関が認証した原文書、変更箇所、最終文書を結合する事により文書を保存する時の扱いが楽になる。

【0529】また、変更文書の各回の変更の認証確認が最終文書から順次溯って復元を行なう必要が無いので、認証の確認が高速で行なえる。

【0530】(第16の実施の形態)本実施形態では、第14の実施形態の変形例である変更文書の認証システムについて説明する。より正確には、図39における変更者#nの変更及び認証手段1006に関する変形例である。

【0531】図51は本発明の第16の実施形態の文書変更を含んだ電子文書の改竄防止システムにおける変更及び認証手段の機能構成及び処理流れを示す図であり、図40と同一部分には同一の符号を付して説明を省略する。

【0532】図51に示す文書変更を含んだ電子文書の

改竄防止システムは、変更者#nの変更及び認証手段1006において、図40の変更者認証手段1025Aに代えて特徴抽出手段1033及び変更者認証手段1034が設けられる他、第14の実施形態と同様に構成されている。

【0533】ここで、特徴抽出手段1033は、変更文書1022の特徴を抽出する手段である。また、変更者認証手段1034は、結合手段1028から出力される結合データを変更者の暗号鍵で暗号化して認証し、認証データ1029を出力する手段である。なお、変更者認証手段1034は、図40の変更者認証手段1025Aと類似するものであって、特徴データ1025A-2の代わりに、結合手段1028により出力される結合データの特徴抽出することなく暗号化するものである。

【0534】次に、以上のように構成された本発明の実施の形態に係る電子文書の改竄防止システムの動作について説明する。

【0535】まず、変更及び認証手段1006に与えられたn-1回目の認証付き変更電子文書1004から、n回目変更変更電子文書1022及び認証データ1027が得られるところまでは第14の実施形態と同様である。

【0536】次に、n回目変更電子文書1022は特徴抽出手段1033に入力される。この特徴抽出手段1033により生成された特徴データは結合手段1028によって、認証データ1027と結合される。この結合手段1028によって結合されたデータは、変更者認証手段1034に与えられ暗号化されて、n回目変更文書の変更者結合認証データ1029が作成される。

【0537】以下、第14の実施形態と同様な処理が行われる。

【0538】上述したように、本発明の実施の形態に係る変更電子文書の改竄防止システム及び方法は、第14の実施形態と同様な構成を有する他、特徴抽出手段1033及び変更者認証手段1034を設けたので、第14の実施形態と同様な効果が得られる他、変更文書本体の改竄を行なうと改竄後の文書から抽出されるべき特徴データが変化し、先に認証用に抽出された特徴データ1033と異なるものになる事によって、変更文書本体の改竄の事実を検出することができる。

【0539】また、一方先に認証用に抽出された特徴データ1033は外部認証機関の認証データ1030A-Aとともに認証機関の秘密鍵1030A-2で暗号化されているので、認証付き変更電子文書1008に付されている認証データ1032Aの改竄は不可能である。従って、たとえ本人であっても外部認証後には文書改竄が不可能になる。

【0540】(第17の実施の形態)本実施形態では、第15の実施形態の変形例である変更文書の認証確認システムについて説明する。より正確には、図45の認証確認手段1040及び1040#n-1に関する変形例であ

る。

【0541】図52は本発明の第17の実施形態の文書変更を含んだ電子文書の改竄防止システムにおける認証確認手段の機能構成及び処理流れを示す図であり、図45と同一部分には同一の符号を付して説明を省略する。

【0542】図52に示す文書変更を含んだ電子文書の改竄防止システムは、認証確認手段1040、1040#n-1及び1043において、分離手段1405Aに代えて分離手段1414Aが設けられる他、第15の実施形態と同様に構成されている。

【0543】次に、以上のように構成された本発明の実施の形態に係る電子文書の改竄防止システムの動作について説明する。

【0544】まず、認証確認手段1040Aにおいて、変更結合認証データ1404Aが得られるところまでは、第15の実施形態と同様である。

【0545】ここで、変更者結合認証データ1404A-Dは、復号化手段1409Aに与えられ、n回目の変更者の公開鍵1408Aにより変更者結合認証データ復号される。復号データはさらに分離手段1414Aによって分離され、特徴データ1410Aと認証データ1407Aとなる。

【0546】以下、第15と同様な処理が行われる。

【0547】なお、認証確認手段1040#n-1及び1043においても、同様な処理が行われる。

【0548】上述したように、本発明の実施の形態に係る変更電子文書の改竄防止システム及び方法は、第15の実施形態と同様な構成を有する他、分離手段1405Aに代えて分離手段1414Aを設けたので、第15の実施形態と同様な効果を得ることができる。

【0549】なお、本発明は、上記各実施の形態に限定されるものでなく、その要旨を逸脱しない範囲で種々に変形することが可能である。

【0550】例えば各実施形態では単に電子文書1とのみ表現するが、この電子文書なるものは電子情報ならば文書に限らず何でもよい。例えば映像データ、音声データ、プログラムソースファイル、プログラム実行ファイル等のバイナリデータをも含む。

【0551】さらに、実施形態では主として公開鍵暗号方式の場合を説明しているが、本発明はこれに限られるものではなく、例えば秘密鍵暗号方式を用いてもよい。

【0552】また、実施形態に記載した手法は、計算機（コンピュータ）に実行させることができるプログラム（ソフトウェア手段）として、例えば磁気ディスク（フロッピーディスク、ハードディスク等）、光ディスク（CD-ROM、DVD等）、半導体メモリ等の記憶媒体に格納し、また通信媒体により伝送して頒布することもできる。なお、媒体側に格納されるプログラムには、計算機に実行させるソフトウェア手段（実行プログラムのみならずテーブルやデータ構造も含む）を計算機内に

構成させる設定プログラムをも含むものである。本装置を実現する計算機は、記憶媒体に記録されたプログラムを読み込み、また場合により設定プログラムによりソフトウェア手段を構築し、このソフトウェア手段によって動作が制御されることにより上述した処理を実行する。

【0553】

【発明の効果】以上詳記したように本発明によれば、作成者本人自身による改竄をも防止した電子文書が提供できるので、重要文書や公的文書など従来は紙でなければ運用出来なかったものに対しても電子文書での運用が可能になり真の意味での電子化を実現させることを可能とした電子文書の改竄防止システム及び方法を提供することができる。

【0554】このように改竄を防止した電子文書化により、遠隔地でも重要文書を瞬時のうちに送達する事ができるようになる。また、電子契約書の実現により、契約書にサインを行う場合でも離れた場所で瞬時のうちにサインを交わす事ができる。電子文書化により文書の保管場所を取らなくなる。電子文書化により文書の検索が可能になる等、その効果は極めて大である。

【0555】また、本発明によれば、電子文書の特徴データからは電子文書の内容を伺い知る事ができないので、企業の秘密文書について外部認証機関の認証を行う事ができ、機密漏洩の危険から免れる事ができる電子文書の改竄防止システム及び方法を提供することができる。

【0556】さらに、本発明によれば、電子文書の特徴データを高速で作成でき、また圧縮率も高いので、特徴データ抽出時間とデータの伝送時間の短縮ができる電子文書の改竄防止システム及び方法を提供することができる。

【0557】さらにまた、本発明によれば、指紋データを使用し暗号鍵および秘密鍵を暗号化する事により本人認証データを盗まれる事が有っても他人にはそのデータを利用できないので、本人認証データの信頼性を非常に高くすることができる電子文書の改竄防止システム及び方法を提供することができる。

【0558】また、本発明によれば、複数人が複数時期に渡って一つの電子文書を作成する場合でも、変更文書を関係者全員で再承認する必要をなくしかつ文書改竄を防止して、紙文書の証拠能力以上の証拠能力を有する電子文書を作成可能とした電子文書の改竄防止システム及び方法を提供することができる。

【0559】このように作製者自身による改竄をも防止した変更電子文書が提供できるので、重要文書や公的文書など従来は紙でなければ運用できなかったものに対しても電子文書上での部分変更の運用が可能となる。また、各種設計資料や、設計図面、製作資料や製作図、試験資料や試験データ、試験結果、検査資料や検査結果など、企業の中で使用される文書で社外に開示をしなくな

い資料について、それらのドキュメントの内容と製作時期、変更内容と変更時期が証明されるので、製品事故などが発生した時の非常に有力な裁判資料として使用できる。とくに、設計工程、製造工程、検査工程の中等で、1枚の紙に複数の時期にわたって内容が追記されていくチェックシート等が裁判の場で正当性を証明できる資料としての電子化を実現する。

【図面の簡単な説明】

【図1】本発明の各実施形態における電子文書の作成システム及び方法の全体的な構成を示す図。

【図2】本発明の第1の実施の形態に係る電子文書の改竄防止システムに適用される文書認証システムのハードウェア構成例を示すブロック図。

【図3】同実施形態の電子文書の改竄防止システムに適用される外部認証システムのハードウェア構成例を示すブロック図。

【図4】同実施形態の電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図。

【図5】同実施形態の電子文書の改竄防止システムの動作を示す流れ図。

【図6】本発明の第2の実施の形態に係る電子文書の改竄防止システムに適用される認証文書確認システムのハードウェア構成例を示すブロック図。

【図7】同実施形態の電子文書の改竄防止システムに適用される認証文書確認システムの機能構成及び処理流れの一例を示す図。

【図8】同実施形態の電子文書の改竄防止システムの動作を示す流れ図。

【図9】本発明の第3の実施の形態の電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図。

【図10】同実施形態の電子文書の改竄防止システムの動作を示す流れ図。

【図11】本発明の第4の実施の形態の電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図。

【図12】同実施形態の電子文書の改竄防止システムの動作を示す流れ図。

【図13】本発明の第5の実施の形態の電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図。

【図14】同実施形態の電子文書の改竄防止システムの動作を示す流れ図。

【図15】本発明の第6の実施の形態の電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図。

【図16】本発明の第7の実施形態の電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図。

【図17】同実施形態の電子文書の改竄防止システムの電子印鑑生成処理を示す流れ図。

【図18】同実施形態の電子文書の改竄防止システムの電子印鑑照合処理を示す流れ図。

【図19】同実施形態の電子文書の改竄防止システムの文書見出し編集処理を示す流れ図。

【図20】本発明の第8の実施の形態の電子文書の改竄防止システムにおける特徴抽出方法を説明するための図。

【図21】同実施形態の電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図。

【図22】同実施形態の電子文書の改竄防止システムの特徴データ抽出の処理の一例を示す流れ図。

【図23】本発明の第9の実施の形態の電子文書の改竄防止システムにおける特徴抽出方法を説明するための図。

【図24】本発明の第10の実施の形態の電子文書の改竄防止システムにおける特徴抽出方法を説明するための図。

【図25】同実施形態の電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図。

【図26】同実施形態の電子文書の改竄防止システムの特徴データ抽出の処理の一例を示す流れ図。

【図27】本発明の第11の実施の形態の電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図。

【図28】同実施形態の電子文書の改竄防止システムの動作を示す流れ図。

【図29】本発明の第12の実施の形態の電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図。

【図30】同実施形態の電子文書の改竄防止システムの動作を示す流れ図。

【図31】本発明の第13の実施の形態の電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図。

【図32】指紋データの一例を示す図。

【図33】指紋データから矩形領域に切り出したデータの一例を示す図。

【図34】マッチングさせるパターンの例の一部分を示した図。

【図35】同実施形態の電子文書の改竄防止システムの動作を示す流れ図。

【図36】本発明の第14～第17の実施形態における文書変更を含んだ電子文書の改竄防止システム及び方法の全体的な構成を示す図。

【図37】本発明の第14の実施形態に係る文書変更を含んだ電子文書の改竄防止システムに適用される文書変更認証システムのハードウェア構成例を示すブロック図。

【図38】同実施形態の文書変更を含んだ電子文書の改竄防止システムに適用される外部認証システムのハードウェア構成例を示すブロック図。

【図39】同実施形態の文書変更を含んだ電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図。

50 図。

【図40】同実施形態の文書変更を含んだ電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図。

【図41】変更者#nの変更及び認証手段における変更者認証手段の構成を示す図。

【図42】外部認証システムにおける外部認証手段の構成を示す図。

【図43】同実施形態の電子文書の改竄防止システムの動作を示す流れ図。

【図44】本発明の第15の実施の形態に係る変更電子文書の改竄防止システムに適用される認証文書確認システムのハードウェア構成例を示すブロック図。

【図45】同実施形態の変更電子文書の改竄防止システムに適用される認証文書確認システムの機能構成ならびに処理流れの一例を示す図。

【図46】認証確認手段1040の詳細構成を示す図。

【図47】認証確認手段1040 #n-1の詳細構成を示す図。

【図48】同実施形態の電子文書の改竄防止システムの動作を示す流れ図。

【図49】同実施形態の認証確認システムにおける認証確認手段1040Aの処理を示す流れ図。

【図50】同実施形態の認証確認システムにおける認証確認手段1040Bの処理を示す流れ図。

【図51】本発明の第16の実施形態の文書変更を含んだ電子文書の改竄防止システムにおける変更及び認証手段の機能構成及び処理流れを示す図。

【図52】本発明の第17の実施形態の文書変更を含んだ電子文書の改竄防止システムにおける認証確認手段の機能構成及び処理流れを示す図。

【図53】電子文書に署名してその同一性を判定する従来の方法を示す図。

【符号の説明】

- 1…電子文書
- 2…特徴抽出手段
- 2T…セパレータテーブル
- 2W…単語配列
- 3…見出し付き特徴データ
- 3H…見出し
- 3D…特徴データ
- 4…秘密鍵
- 5…暗号化手段
- 6…見出し付き暗号データ
- 6H…見出し
- 6D…暗号データ
- 7…見出し付き認証データ
- 7H…見出し
- 7D…暗号データ
- 7A…外部認証データ
- 8…秘密鍵

- 9…暗号化手段
- 10…合成データ
- 10H…見出し
- 10D…暗号データ
- 11…合成データ
- 11H…見出し
- 11D…暗号データ
- 12…認証付電子文書
- 13…公開鍵
- 14…復号化手段
- 15…見出し付き認証データ
- 15H…見出し
- 15D…暗号データ
- 15A…外部認証データ
- 15A-D…日付認証
- 16…公開鍵
- 17…復号化手段
- 18…見出し付き特徴データ
- 18H…見出し
- 18D…特徴データ
- 19…電子文書
- 20…特徴抽出手段
- 21…特徴データ
- 22…照合手段
- 22-J…同一性判定
- 23…見出し付き認証データ
- 23H…見出し
- 23D…暗号データ
- 23A…外部認証データ
- 24…秘密鍵
- 25…暗号化手段
- 26…見出し付き暗号データ
- 26H…見出し
- 26D…暗号データ
- 27…見出し付き暗号データ
- 27H…見出し
- 27D…暗号データ
- 28…認証付電子文書
- 29…公開鍵
- 30…復号化手段
- 31…見出し付き認証データ
- 31H…見出し
- 31D…暗号データ
- 31A…外部認証データ
- 31A-D…日付認証
- 32…見出し付き認証データ
- 32H…見出し
- 32D…暗号データ
- 32A…外部認証データ
- 33…秘密鍵

3 4 …暗号化手段
 3 5 …見出し付き暗号データ
 3 5 H …見出し
 3 5 D …暗号データ
 3 6 …見出し付き認証データ
 3 6 H …見出し
 3 6 D …暗号データ
 3 6 A …外部認証データ
 3 7 …秘密鍵
 3 8 …暗号化手段
 3 9 …見出し付き暗号データ
 3 9 H …見出し
 3 9 D …暗号データ
 4 0 …見出し付き暗号データ
 4 0 H …見出し
 4 0 D …暗号データ
 4 1 …認証付電子文書
 4 2 …公開鍵
 4 3 …復号化手段
 4 4 …見出し付き認証データ
 4 4 H …見出し
 4 4 D …暗号データ
 4 4 A …外部認証データ
 4 4 A - D …日付認証
 4 5 …公開鍵
 4 6 …復号化手段
 4 7 …見出し付き認証データ
 4 7 H …見出し
 4 7 D …暗号データ
 4 7 A …外部認証データ
 4 7 A - D …日付認証
 4 8 …公開鍵
 4 9 …復号化手段
 5 0 …見出し付き特徴データ
 5 0 H …見出し
 5 0 D …特徴データ
 5 1 …特徴抽出手段
 5 2 …特徴データ
 5 3 …照合手段
 5 3 - J …同一性判定
 5 4 …印影
 5 5 …特徴抽出手段
 5 6 …特徴データ
 5 8 …暗号化手段
 5 9 …暗号化印影
 6 0 …電子印鑑
 6 1 …日付署名印影情報
 6 2 …整形手段
 6 3 …文書表示手段
 6 4 …指紋読取り機

6 5 …指紋
 6 6 …特徴抽出手段
 6 6 S …切り出し手段
 6 6 S D …データ
 6 6 M …マッチング手段
 6 6 P …パターン
 6 6 D …1 桁分データ
 6 7 …特徴データ
 6 8 …パスワード
 10 6 9 …氏名・I D
 7 0 …暗号鍵生成手段
 7 1 …暗号鍵
 7 2 …乱数発生器
 7 3 …秘密鍵公開鍵生成手段
 7 4 …秘密鍵
 7 5 …公開鍵
 7 6 …暗号化手段
 7 7 …暗号化秘密鍵
 7 8 …本人認証データ
 20 7 8 F …指紋
 7 8 S …暗号化秘密鍵
 7 8 K …暗号化暗号鍵
 7 8 P …パスワード
 7 8 N …氏名・I D
 7 9 …表示手段
 8 0 …照合手段
 8 1 …照合手段
 8 2 …判定ロジック
 8 3 …復号手段
 30 8 4 …暗号鍵
 8 5 …照合手段
 8 6 …復号手段
 8 7 …指紋データ抽出手段
 8 7 F …原指紋データ
 8 7 A …境界抽出手段
 8 7 E …エンボス手段
 8 7 L …輪郭抽出手段
 8 7 B …2 値化
 9 7, 9 8 …記録媒体
 40 9 9 …外部認証機関
 1 0 0 …ネットワーク
 1 0 1 …文書認証システム
 1 0 2 …外部認証システム
 1 0 3 …認証文書確認システム
 1 1 0 …計算機
 1 1 1 …表示装置
 1 1 2 …入力装置
 1 1 3 …印刷装置
 1 1 4 …外部記憶装置
 50 1 1 5 …スキャナ

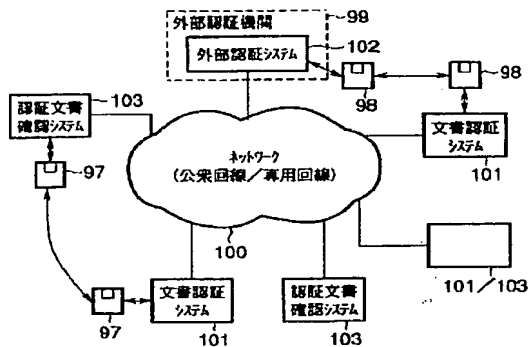
116…CPUバス
 117…CPU
 118…ROM
 119…RAM
 120, 121, 122, 123, 124, 125, 126, 127…インターフェース手段
 128…ハードディスク装置
 129…通信装置
 130…プログラム格納部
 131…データ格納部
 132…作業領域
 133…文書認証プログラム
 134…外部認証プログラム
 135…認証文書確認プログラム
 1001…変更履歴付電子文書
 1002…原電子文書
 1002B…認証確認対象の原電子文書
 1003…変更箇所
 1004…変更電子文書
 1005…分離手段
 1006…変更及び認証手段
 1007…変更箇所
 1007B… n 回変更箇所
 1007B $\#n-1$ … $n-1$ 回変更箇所
 1008…変更電子文書
 1008B…認証確認対象の変更電子文書
 1009…結合手段
 1010…変更箇所
 1011…変更履歴付電子文書
 1011B…認証確認対象の変更履歴付電子文書
 1020…変更電子文書
 1021…変更手段
 1022…変更電子文書
 1023…差分抽出手段
 1024…変更箇所
 1025A, 1025B…変更者認証手段
 1025A-1…特徴抽出手段
 1025A-2…特徴データ
 1025A-3…変更者 $\#n$ 秘密鍵
 1025A-4…暗号化手段
 1026A, 1026B…変更者認証データ
 1026A-H…見出し
 1026A-D…暗号データ
 1027…認証データ
 1027 $\#n-1$ …認証データ
 1028…結合手段
 1029…結合認証データ
 1030A, 1030B…外部認証手段
 1030A-A…外部認証データ
 1030A-1…結合手段

1030A-2…外部秘密鍵
 1030A-3…暗号化手段
 1031A, 1031B…認証データ
 1031A-D…暗号データ
 1031A-H…見出し
 1032A, 1032B…認証データ
 1033…特徴抽出手段
 1034…変更者認証手段
 1040…認証確認手段
 1040A, 1040B…認証確認手段
 1040 $\#n-1$ …認証確認手段
 1041…日付認証
 1041 $\#n-1$ …日付認証
 1042…同一性判定
 1042 $\#n-1$ …同一性判定
 1043…認証確認(繰返し)
 1044…認証確認手段
 1045…日付認証
 1046…同一性判定
 1097, 1098…記録媒体
 1099…外部認証機関
 1100…ネットワーク
 1101…文書認証システム
 1102…外部認証システム
 1103…文書変更認証システム
 1104…認証文書確認システム
 1110…計算機
 1111…表示装置
 1112…入力装置
 1113…印刷装置
 1114…外部記憶装置
 1115…スキャナ
 1116…CPUバス
 1117…CPU
 1118…ROM
 1119…RAM
 1120～1127…インターフェイス手段
 1128…ハードディスク装置
 1129…通信装置
 1130…プログラム格納部
 1131…データ格納部
 1132…作業領域
 1133…文書変更認証プログラム
 1134…外部認証プログラム
 1135…認証文書確認プログラム
 1401A…認証データ
 1401A-D…暗号データ
 1401A-H…見出し
 1402A…外部認証機関の公開鍵
 1403A…復号化手段

85

1404A…変更者結合認証データ
 1404A-D…変更者結合認証データ
 1404A-D1…変更者認証データ
 1404A-D2…外部認証データ
 1404A-H…見出し
 1405A…分離手段
 1406A…変更者認証データ
 1407A…以前の認証データ
 1408A…変更者の公開鍵
 1410A…特徴データ
 1411A…特徴抽出手段
 1412A…特徴データ

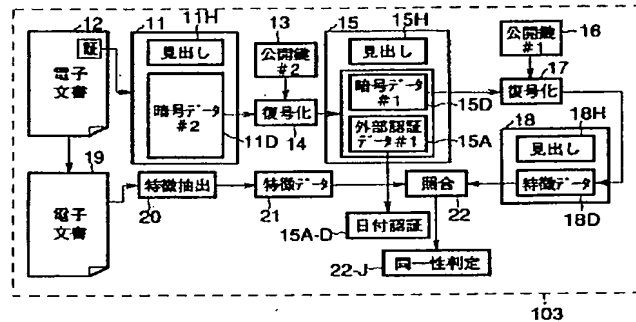
【図1】



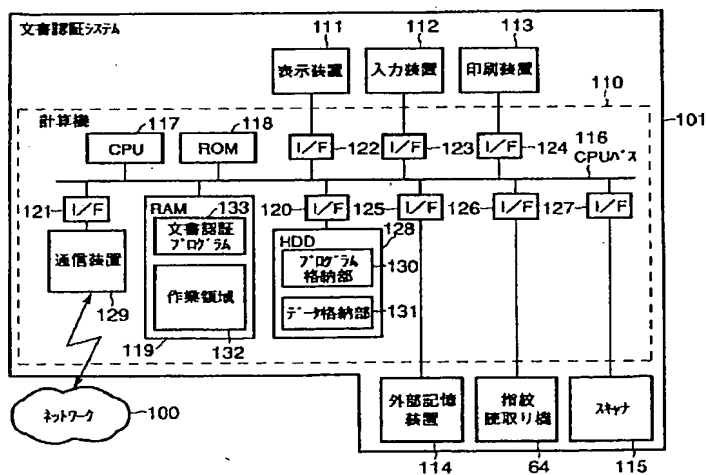
86

* 1413A, 1413B…照合手段
 1414A…分離手段
 S…電子文書データ並び
 S1, S2, S3…電子文書データ並び部分
 S_sum…合計値
 S_stream…合計データ並び
 IS…間隔を置いたデータ並び
 IS1, IS2, IS3…間隔を置いたデータ並び部分
 IS_sum[0], ..., IS_sum[255]…
 10 間隔を置いたデータの合計値の配列
 IS_stream…間隔を置いた合計データ並び
 * i, j…カウンタ

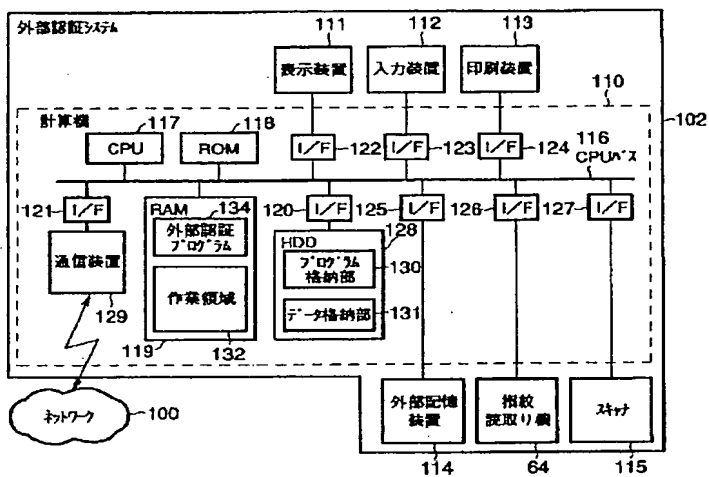
【図7】



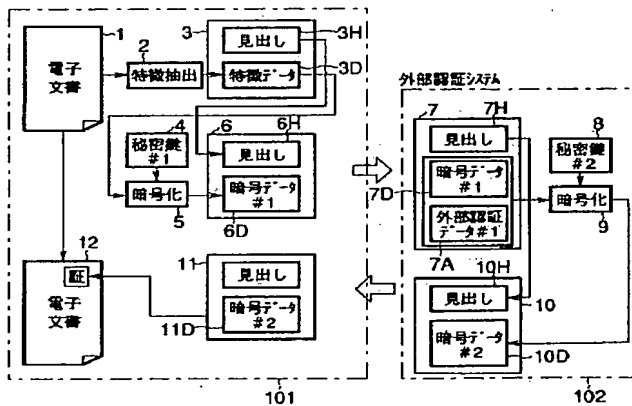
【図2】



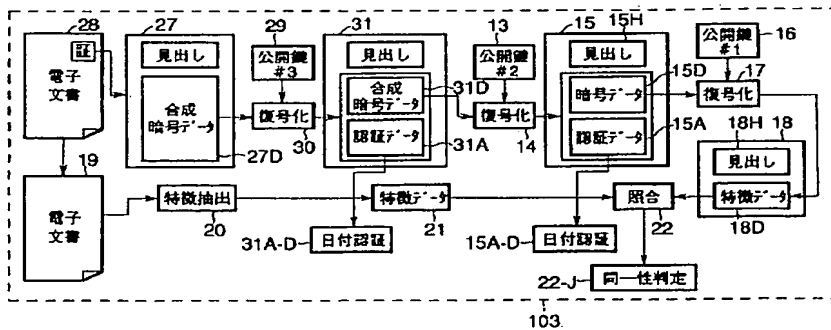
【図3】



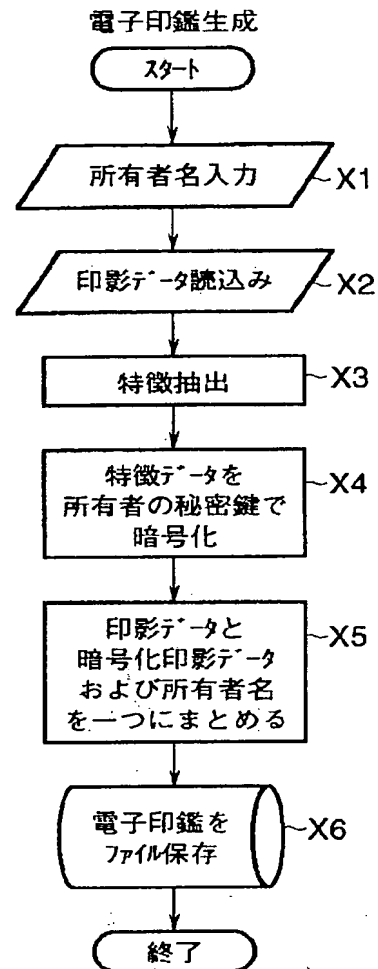
【図4】



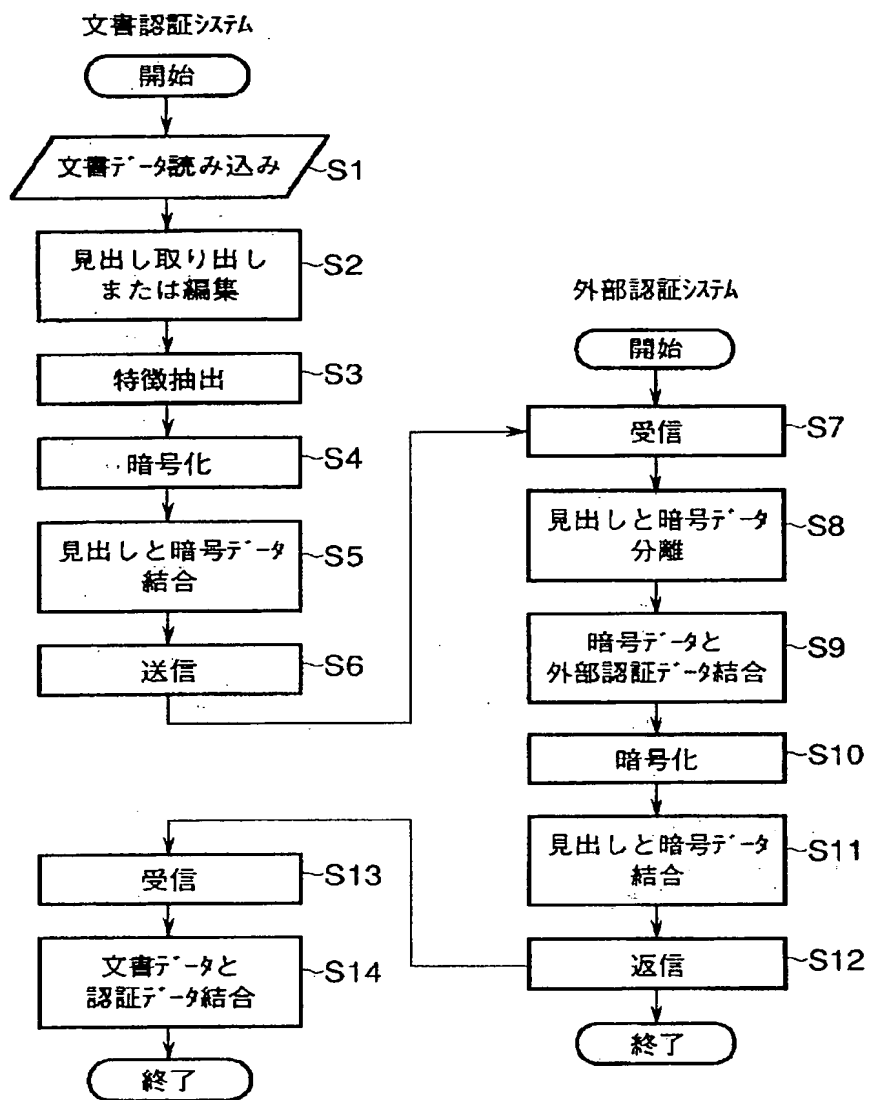
【図11】



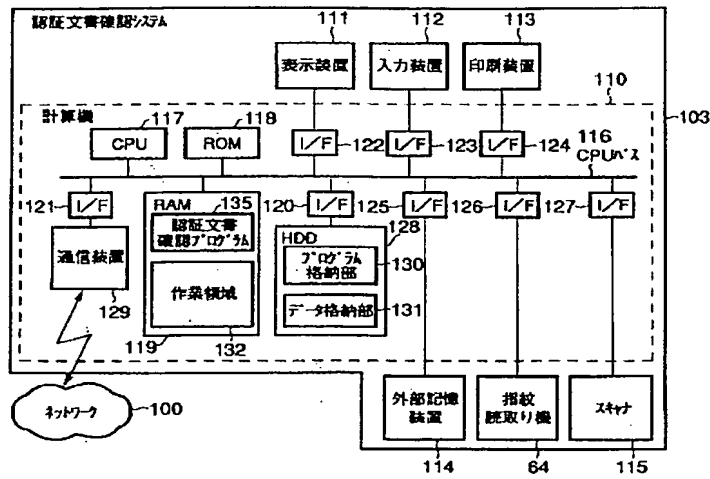
【図17】



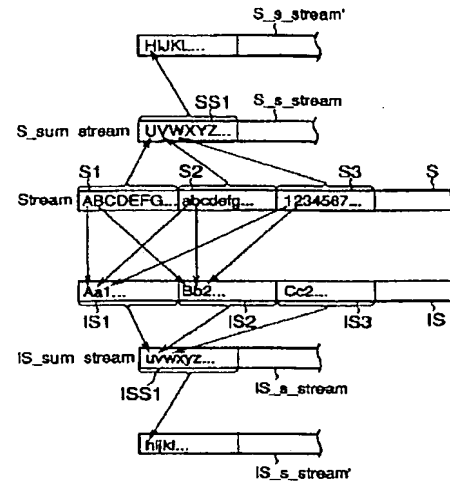
【図5】



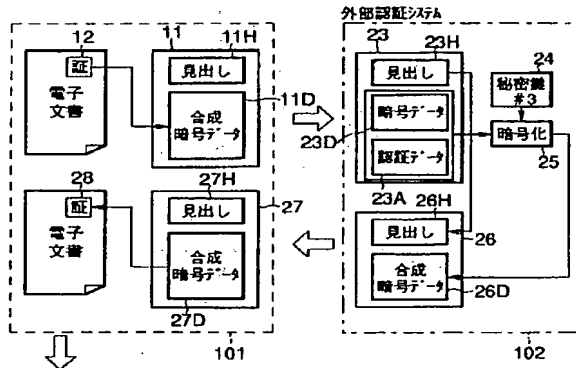
【図6】



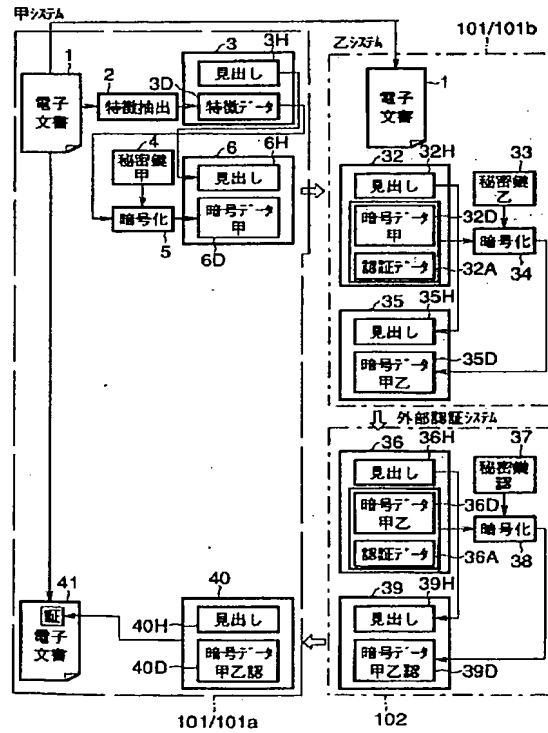
【図23】



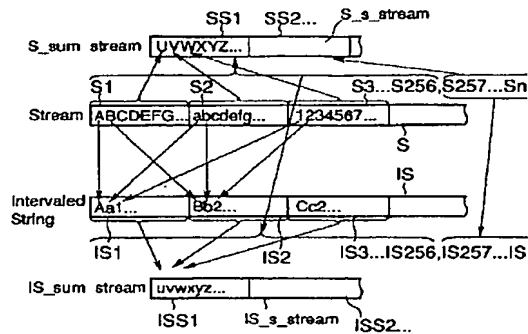
【図9】



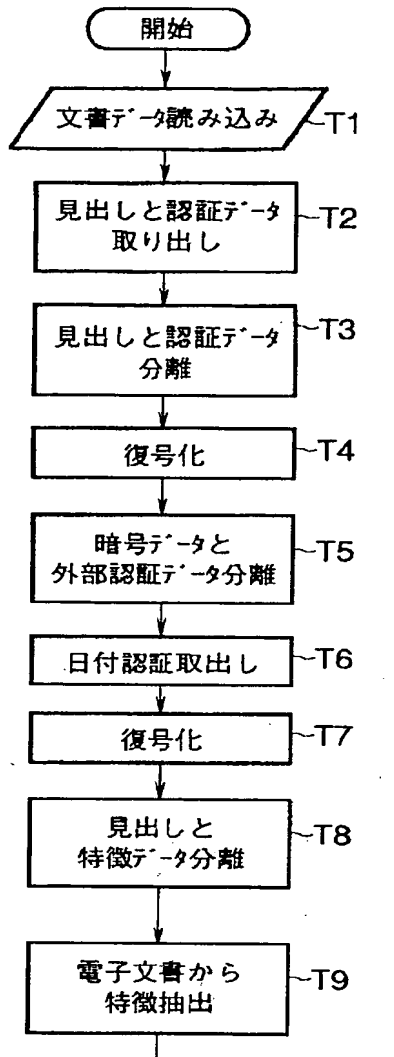
【図13】



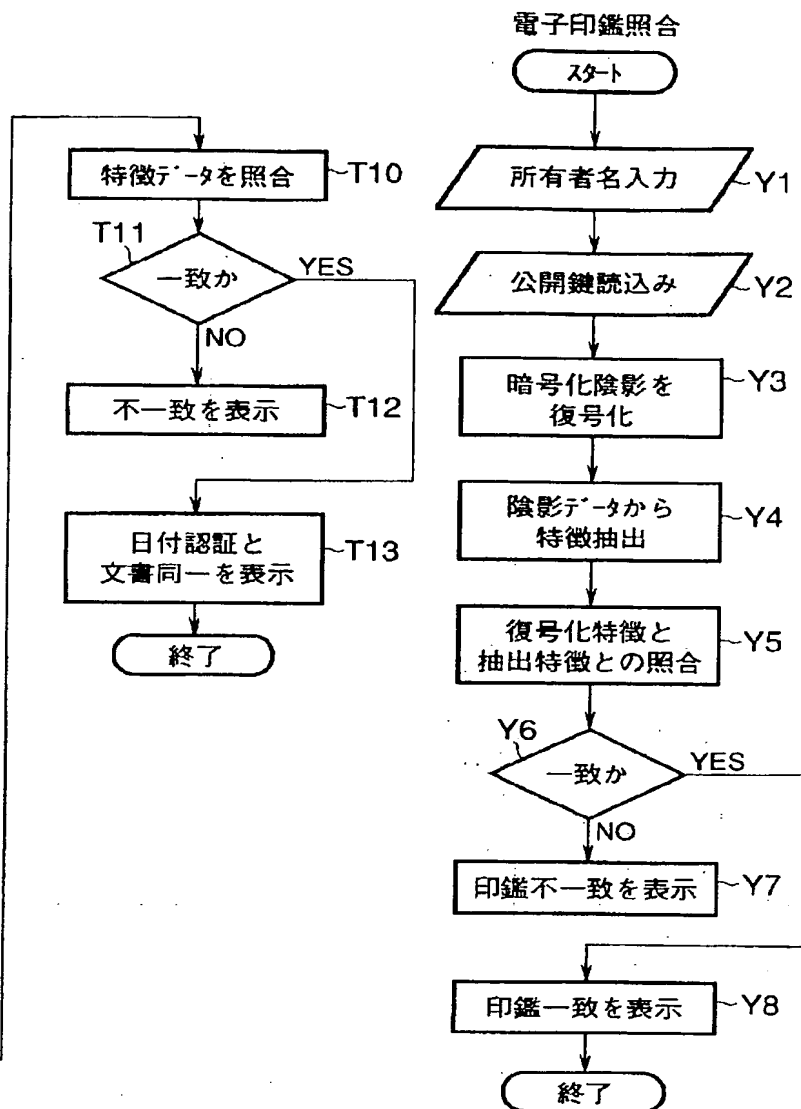
【図20】



【図8】

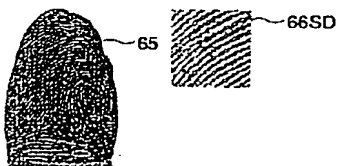


【図18】

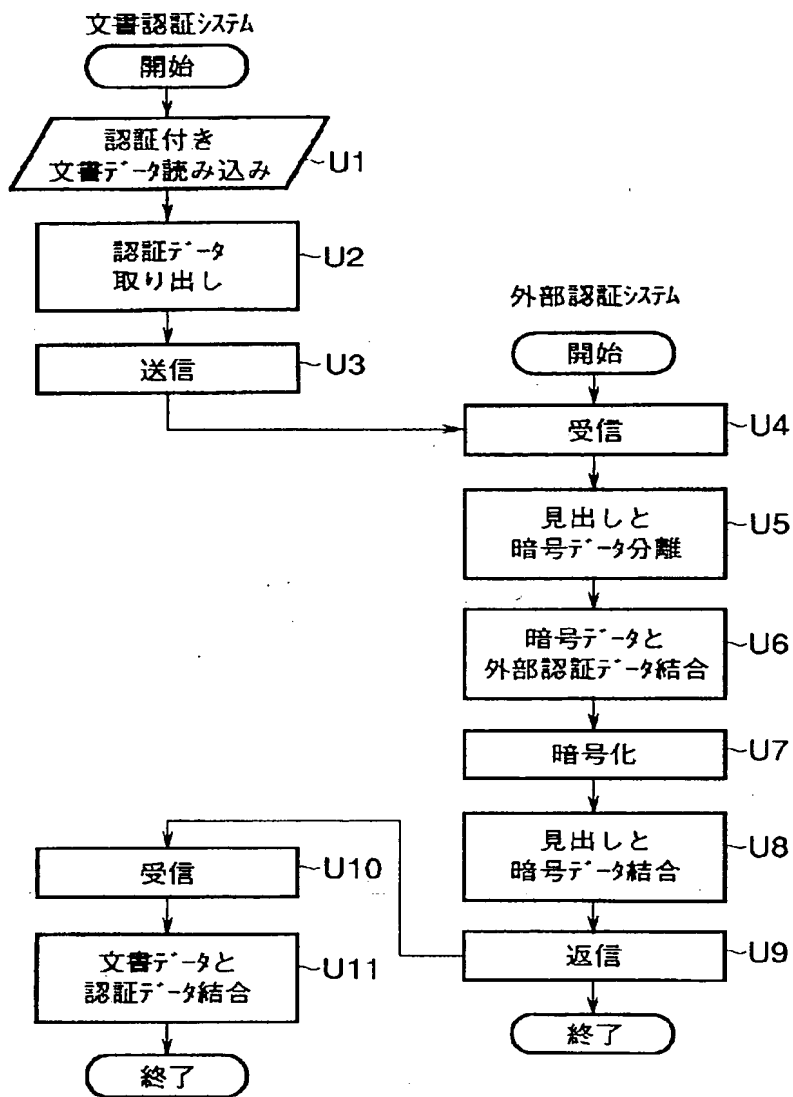


【図32】

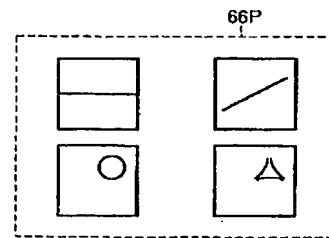
【図33】



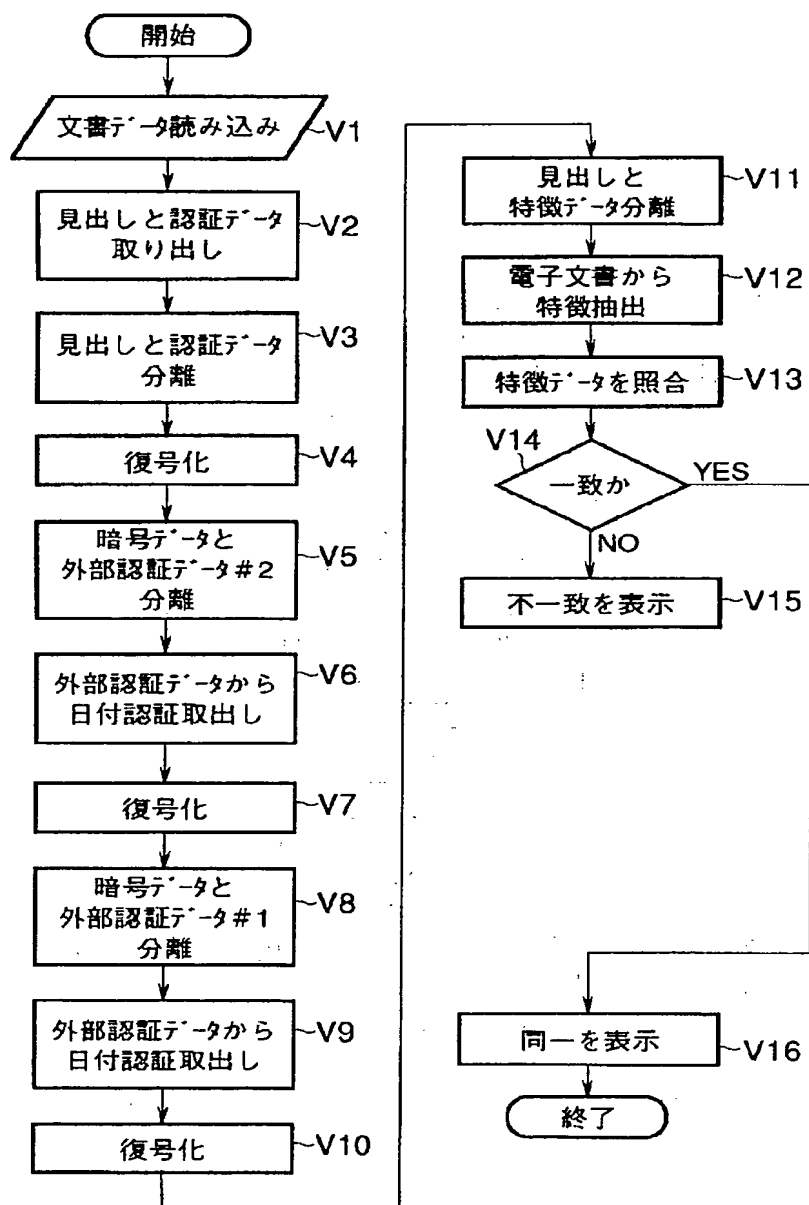
【図10】



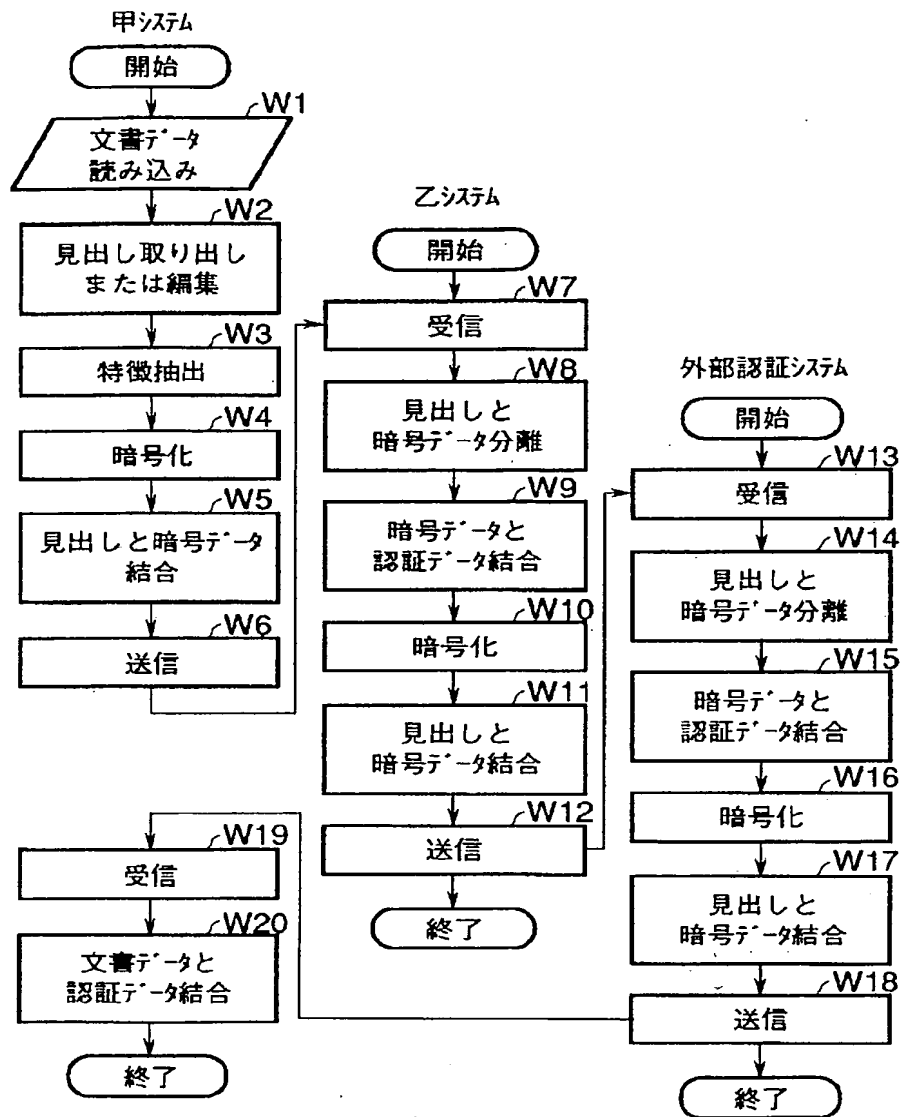
【図34】



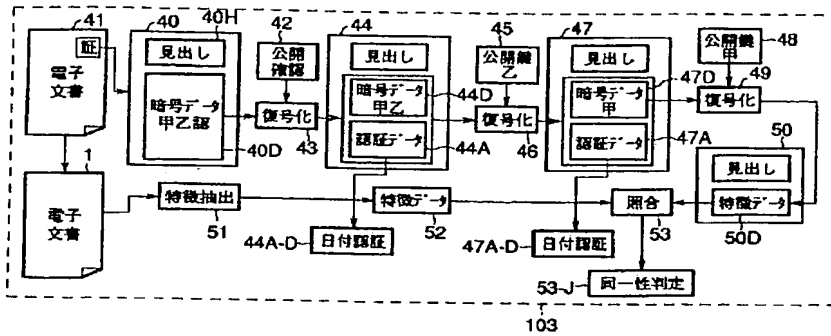
【図12】



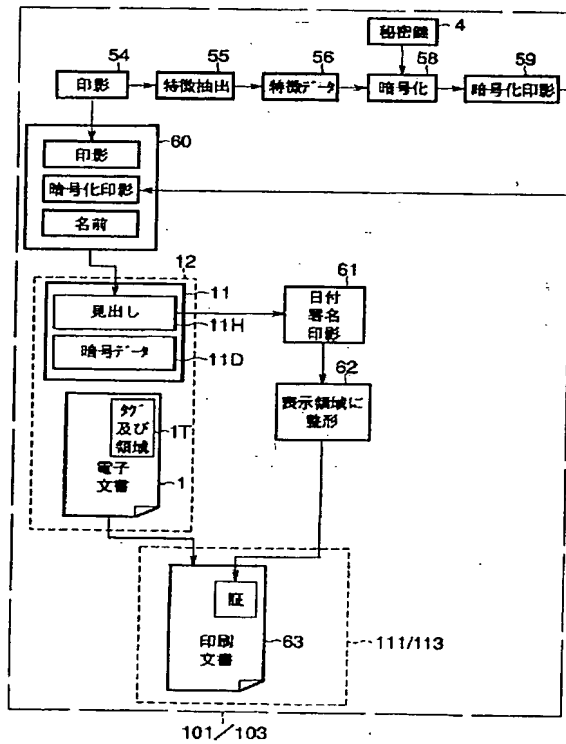
【図14】



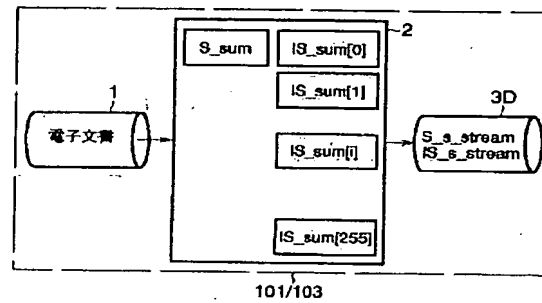
【図15】



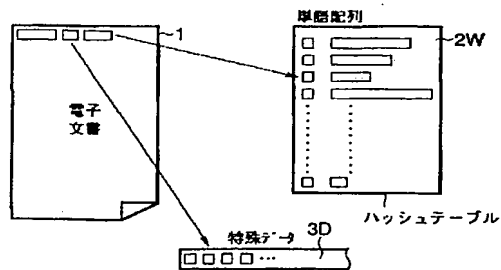
【図16】



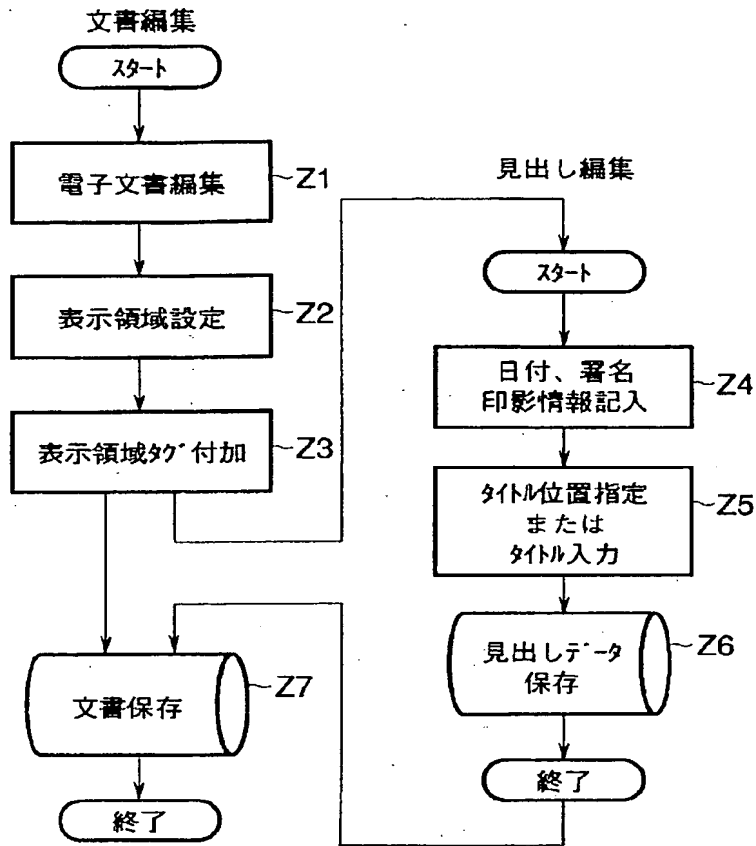
【図21】



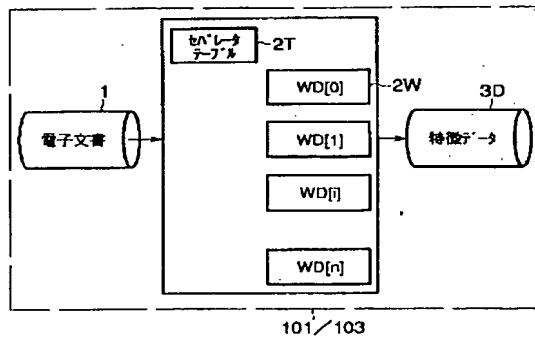
【図24】



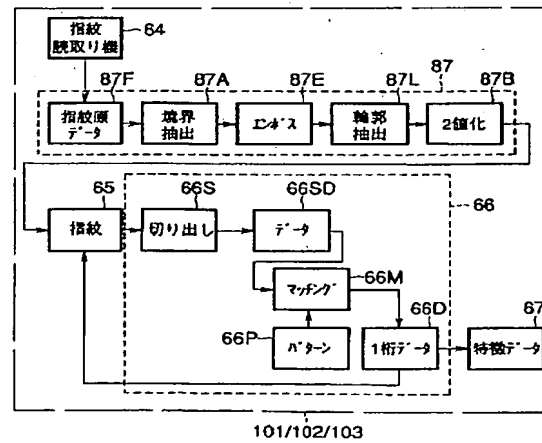
【図19】



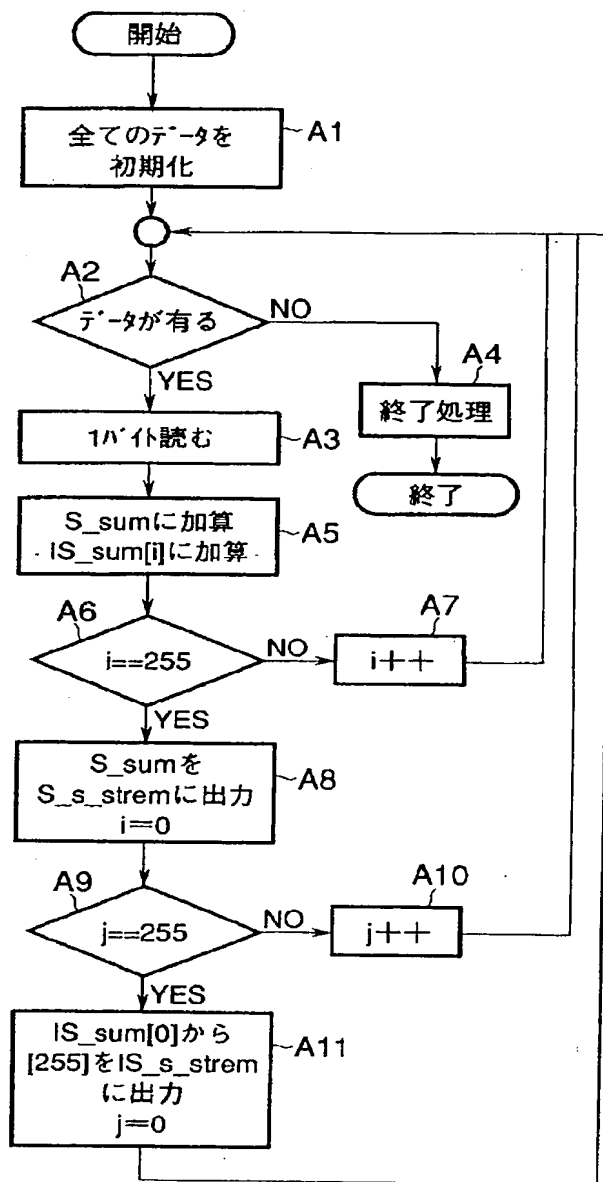
【図25】



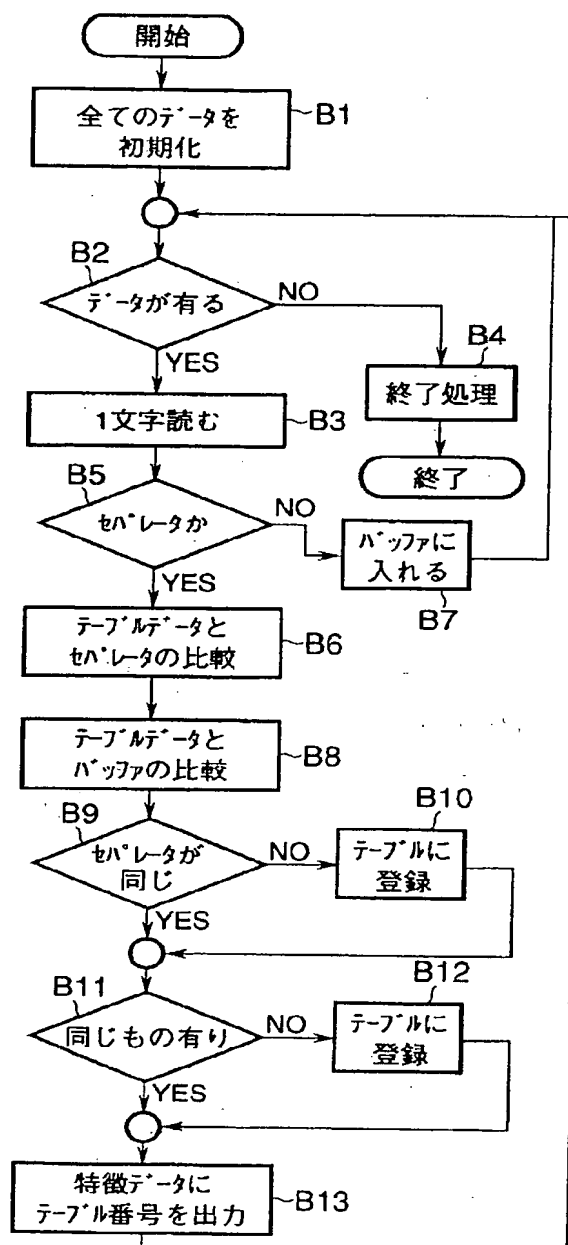
【図31】



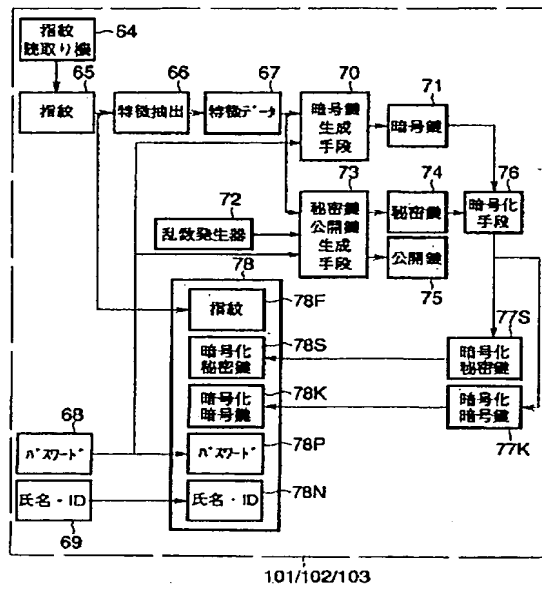
【図22】



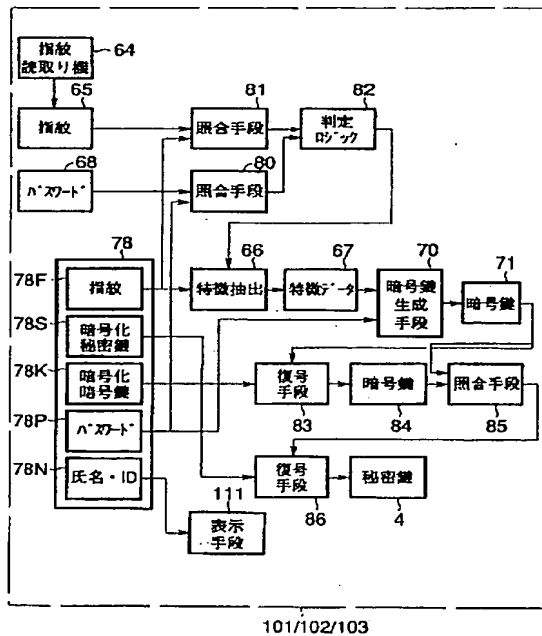
【図26】



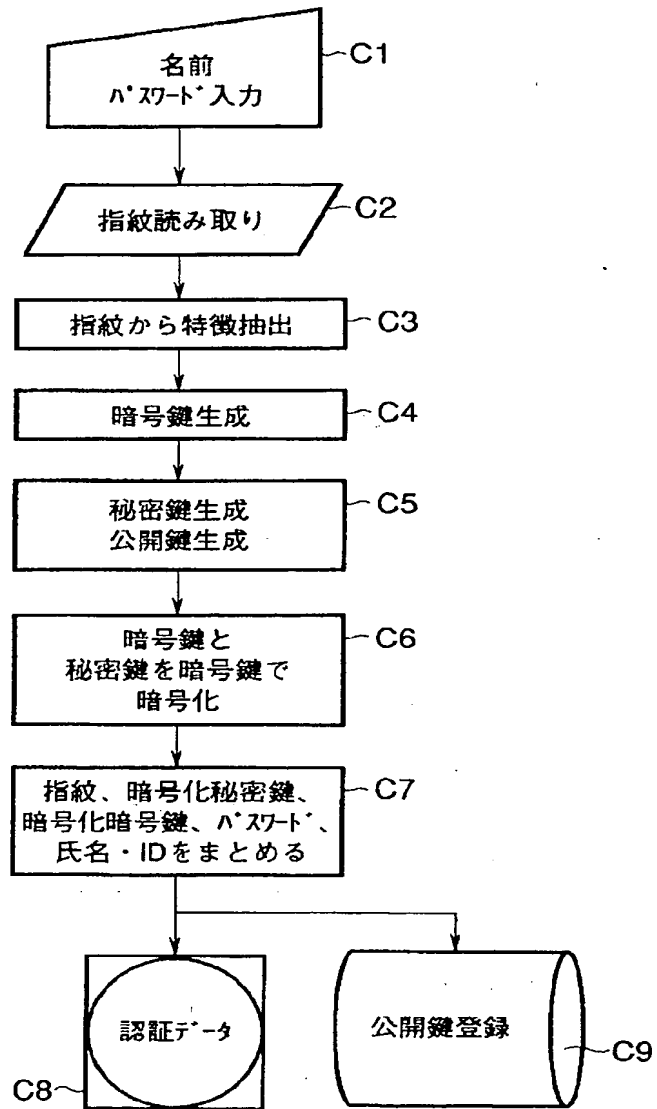
【図27】



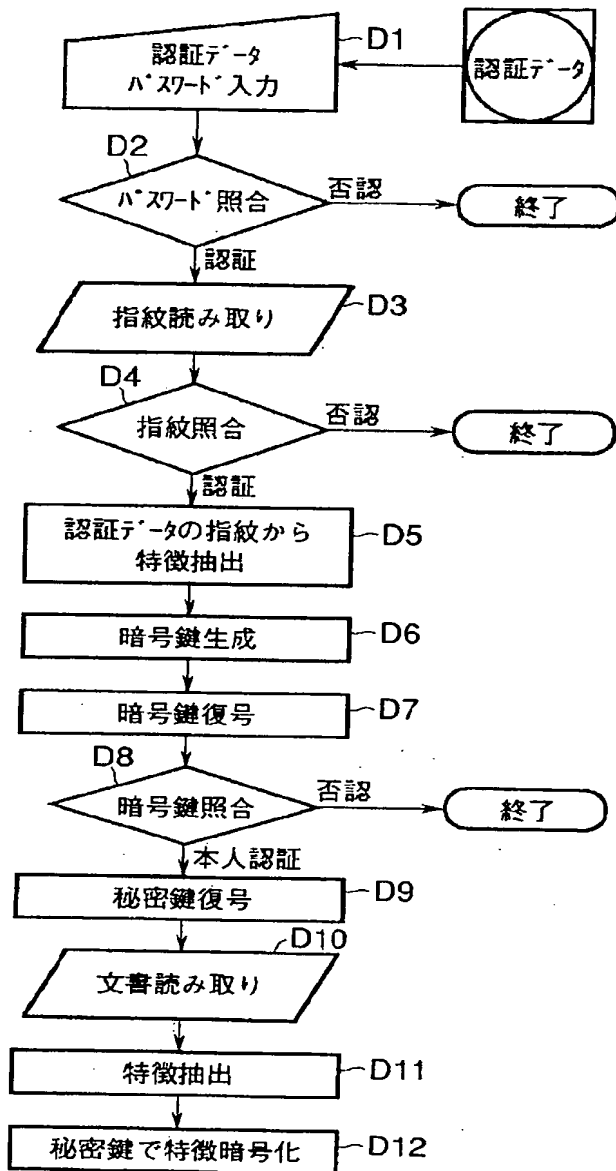
【図29】



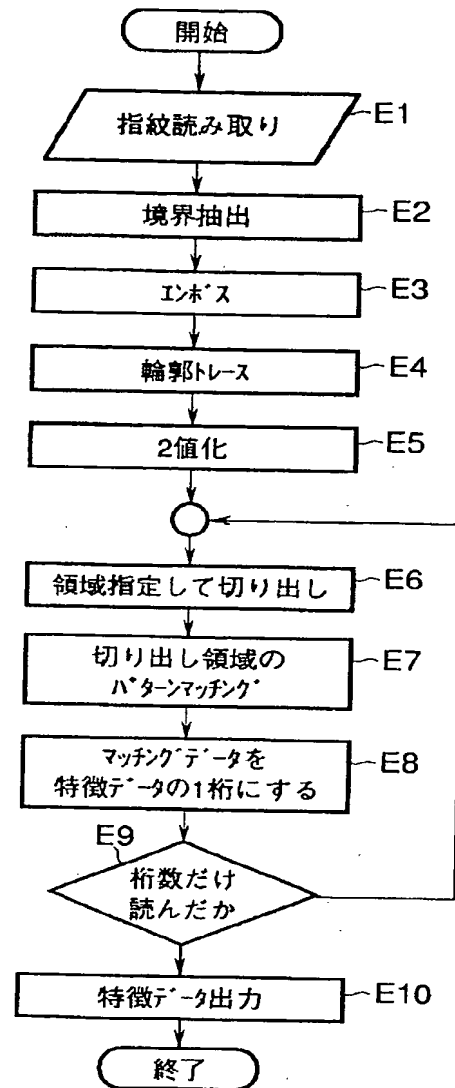
【図28】



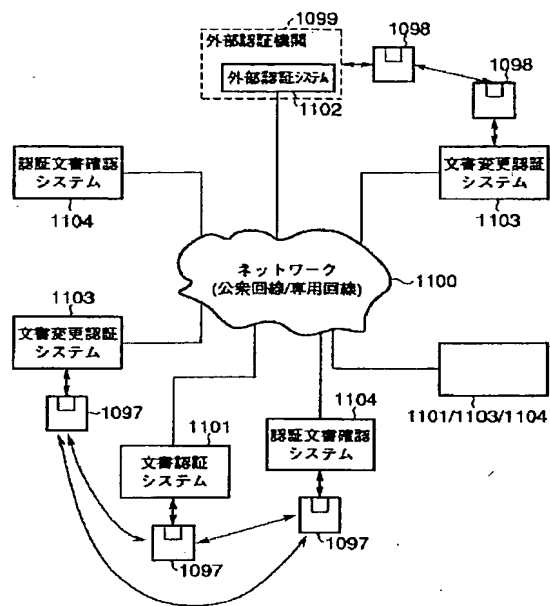
【図30】



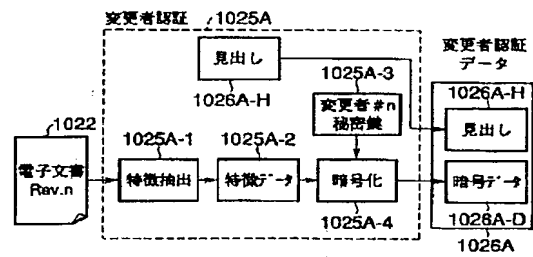
【図35】



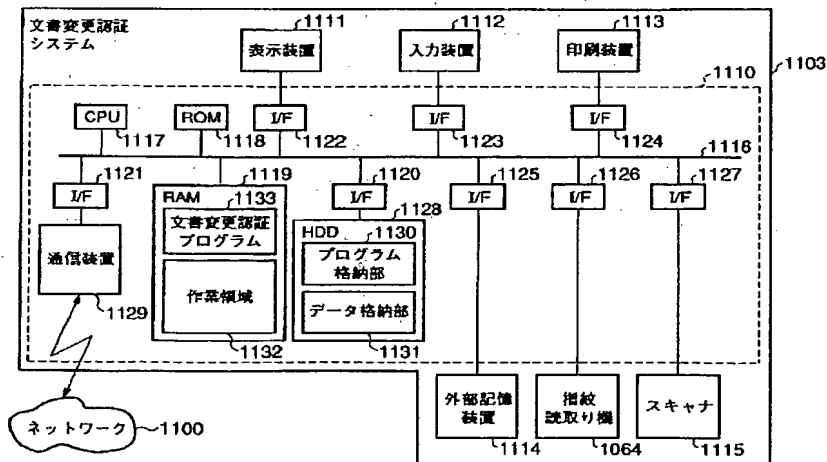
【図36】



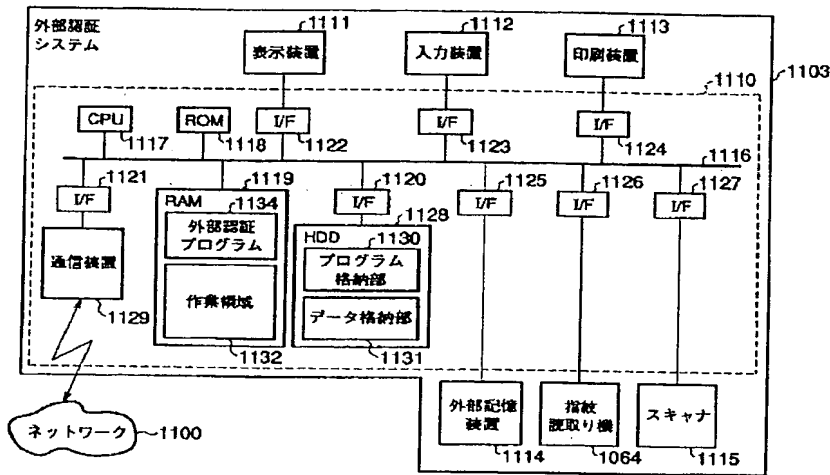
【図41】



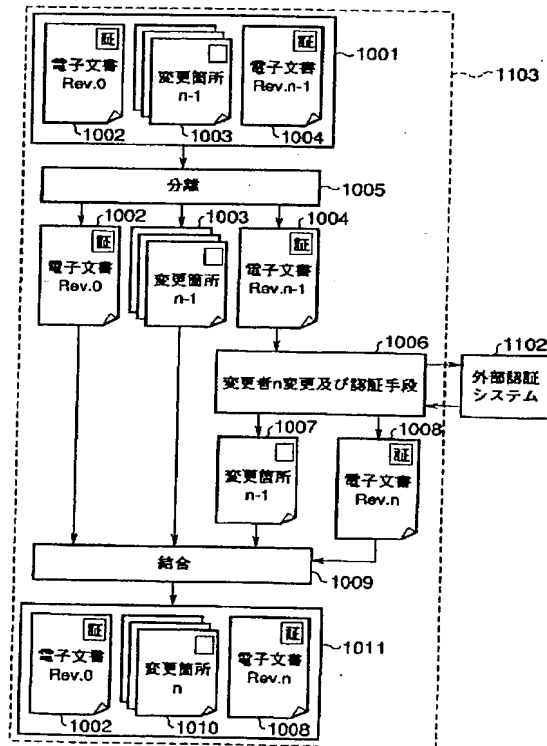
【図37】



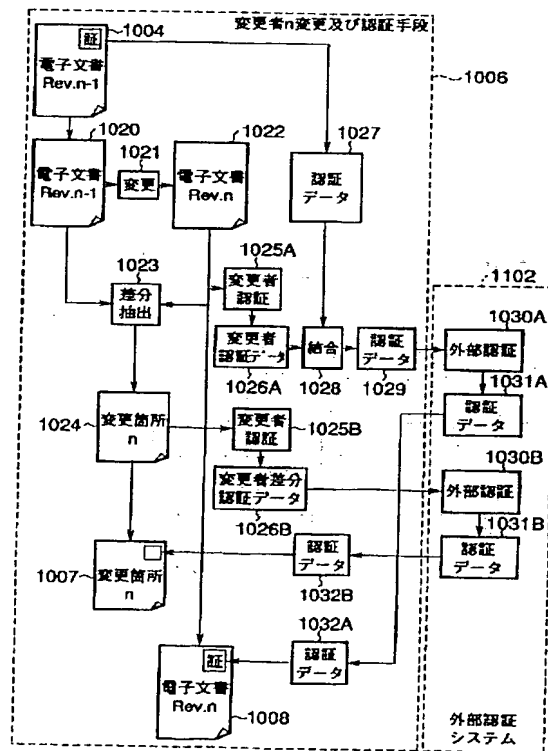
【図38】



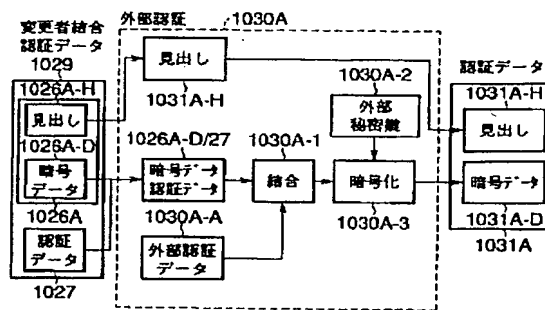
【図39】



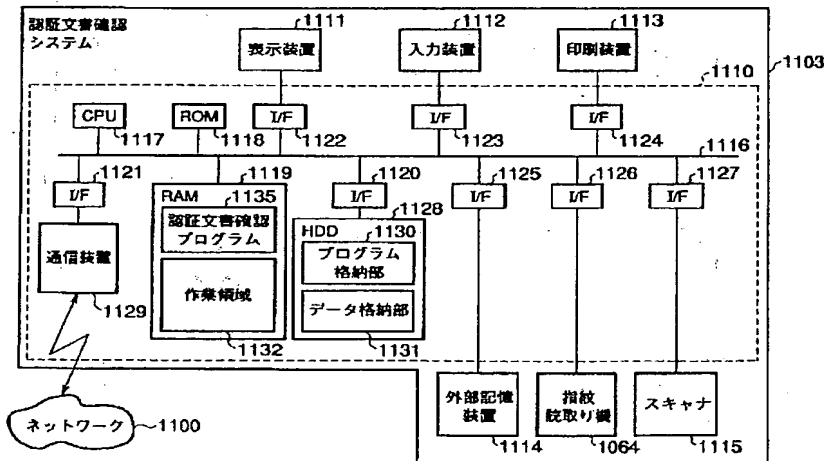
【図40】



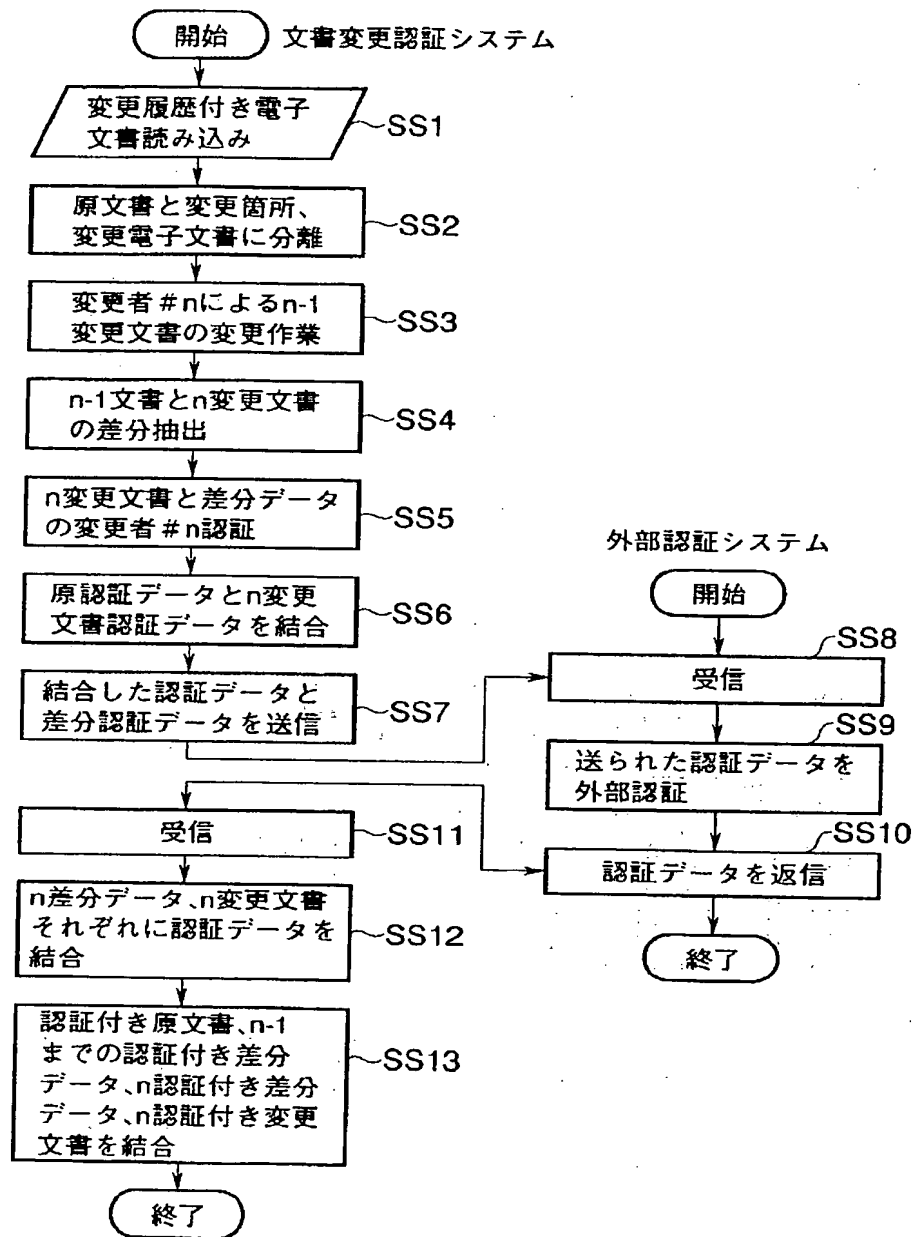
【図42】



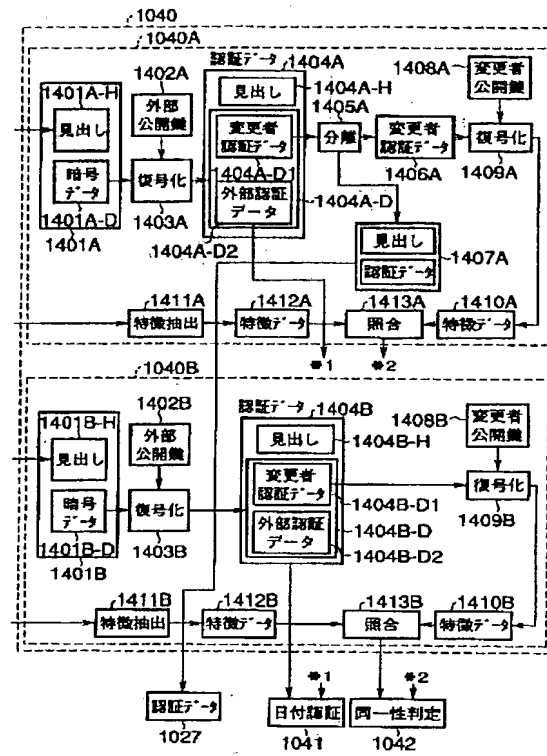
【図44】



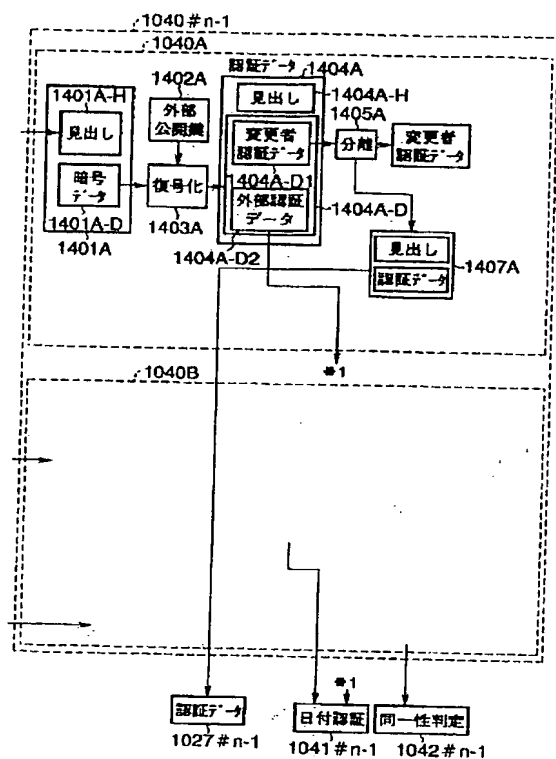
【図43】



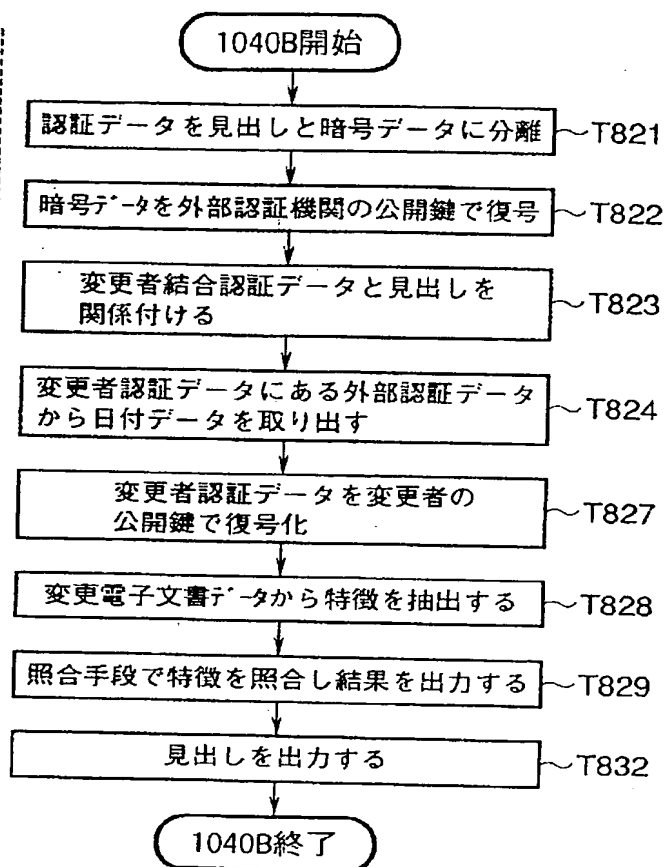
【図46】



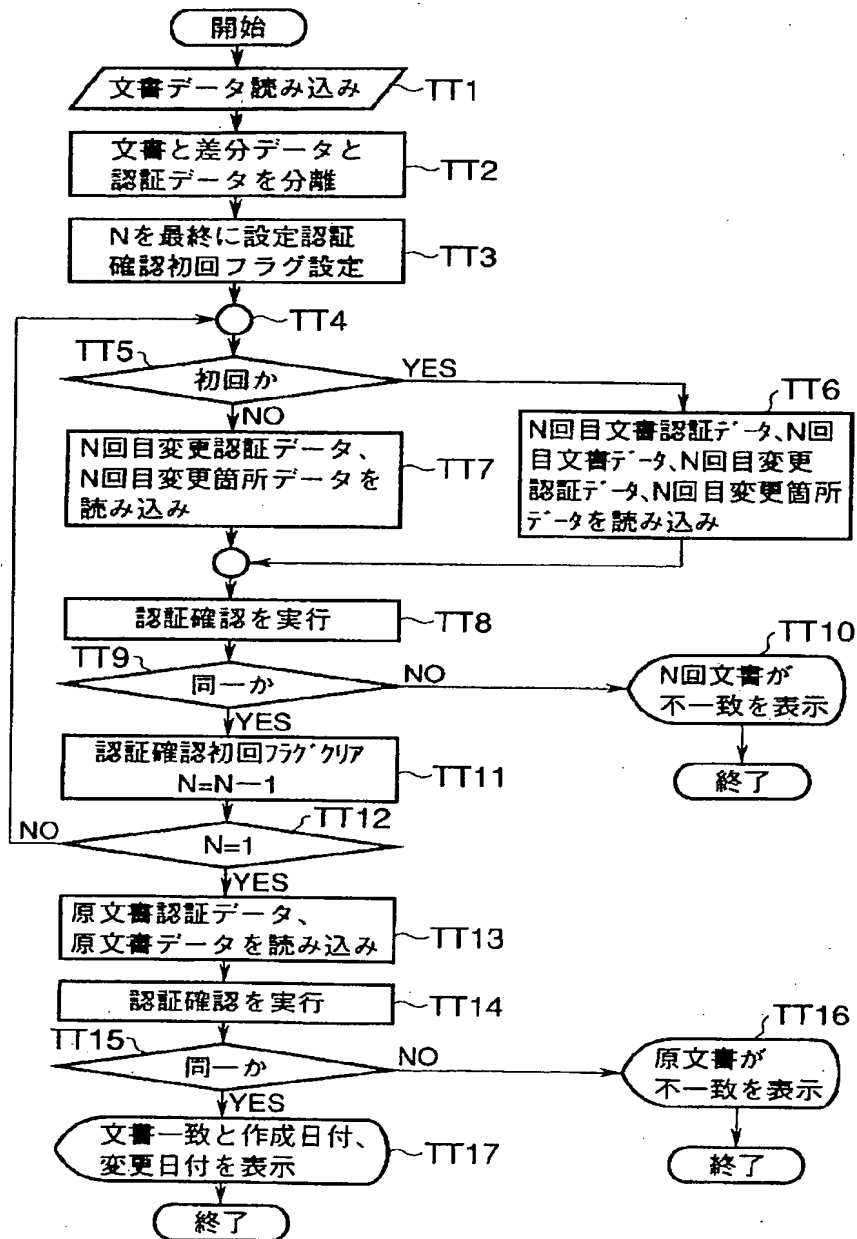
【図47】



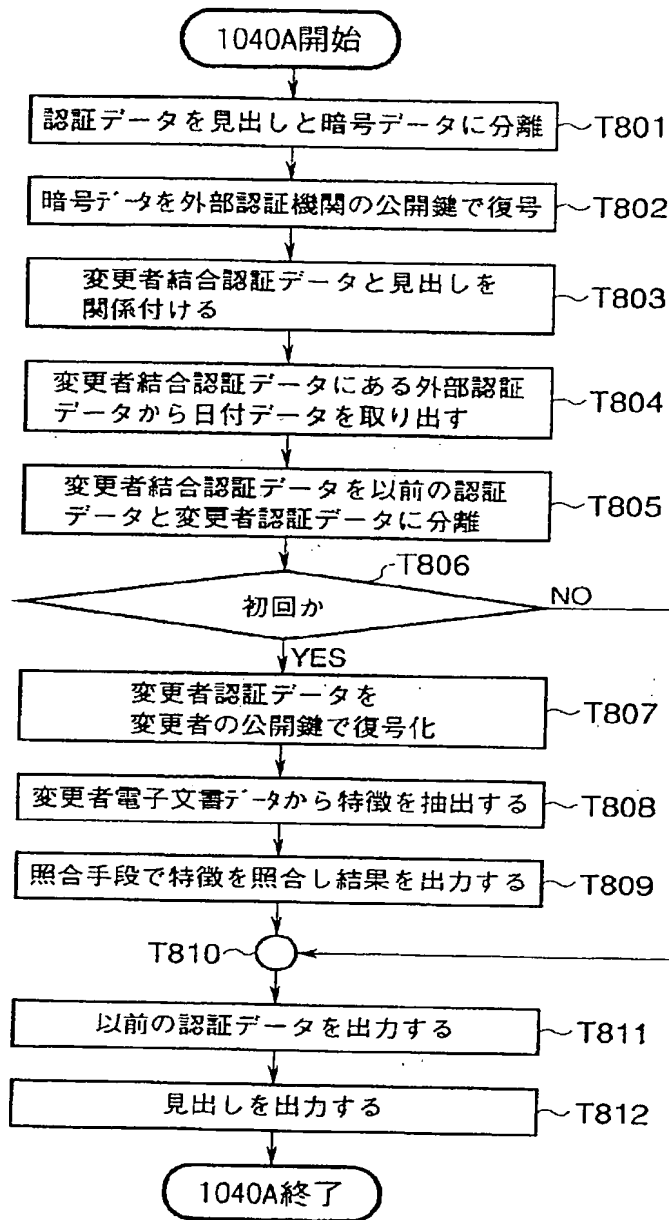
【図50】



〔図48〕



【図49】



【図53】

